RSAC 2025 Conference

Many Voices.
One Community.

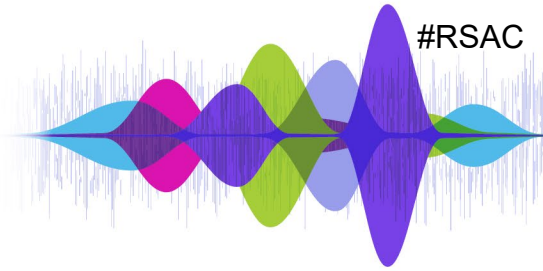
SESSION ID: NCS-W08

Enterprise Security Evolution: The Blindingly Fast & The Glacially Slow

Vern Paxson, Co-Founder and Chief Scientist, Corelight Inc.

Professor of the Graduate School, UC Berkeley

vern@corelight.com / vern@berkeley.edu



Disclaimer

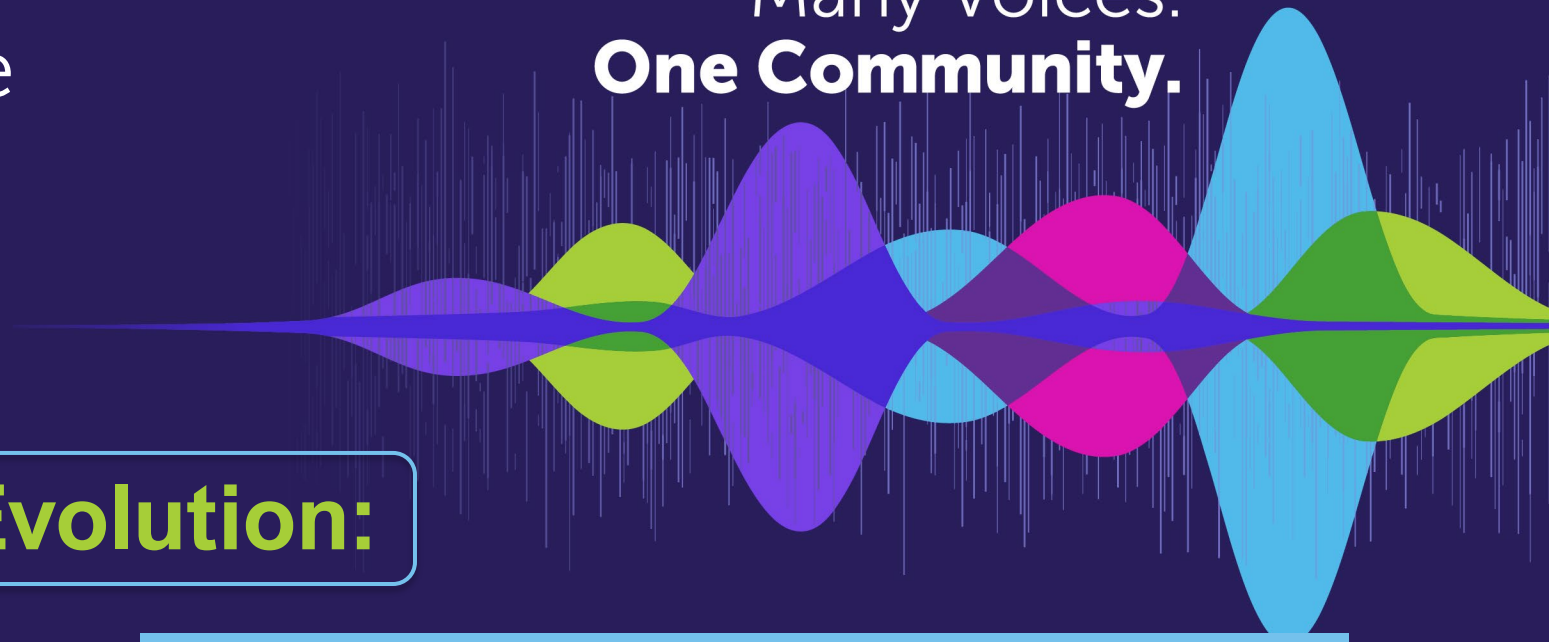
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

Many Voices.
One Community.



SESSION ID: NCS-W08

Enterprise Security Evolution: The Blindingly Fast & The Glacially Slow

How has security – attacks & defenses – changed over time (decades) ?

Vern Paxson, Co-Founder and Chief Scientist, Corelight Inc.

Professor of the Graduate School, UC Berkeley

vern@corelight.com / vern@berkeley.edu

April 30, 2025

RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: NCS-W08

Enterprise Security Evolution: The Blindingly Fast & The Glacially Slow

When it changes, is it sudden?
Predictable? Takes forever?

Vern Paxson, Co-Founder and Chief Scientist, Corelight Inc.

Professor of the Graduate School, UC Berkeley

vern@corelight.com / vern@berkeley.edu

April 30, 2025

RSAC 2025 Conference

Many Voices.
One Community.

Overall story:
1) Very hard to predict when things will significantly change – both attacks & defenses

SESSION ID: NCS-W08

Enterprise Security Evolution: The Blindingly Fast & The Glacially Slow

Vern Paxson, Co-Founder and Chief Scientist, Corelight Inc.

Professor of the Graduate School, UC Berkeley

vern@corelight.com / vern@berkeley.edu

April 30, 2025

RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: NCS-W08

Enterprise Security Evolution: The Blindingly Fast & The Glacially Slow

Overall story:

1) Very hard to predict when things will significantly change – both attacks & defenses
2) What's happening *elsewhere* might not tell you anything about what's happening for **you**

Vern Paxson, Co-Founder and Chief Scientist, Corelight Inc.

Professor of the Graduate School, UC Berkeley

vern@corelight.com / vern@berkeley.edu

April 30, 2025

RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: NCS-W08

Enterprise Security Evolution: The Blindingly Fast & The Glacially Slow

Overall story:

1) Very hard to predict when things will significantly change – both attacks & defenses
2) What's happening *elsewhere* might not tell you anything about what's happening for **you**
3) ⇒ To know what's happening, you need to do your **own** *ongoing* measurements

Vern Paxson, Co-Founder and Chief Scientist, Corelight Inc.

Professor of the Graduate School, UC Berkeley

vern@corelight.com / vern@berkeley.edu

April 30, 2025

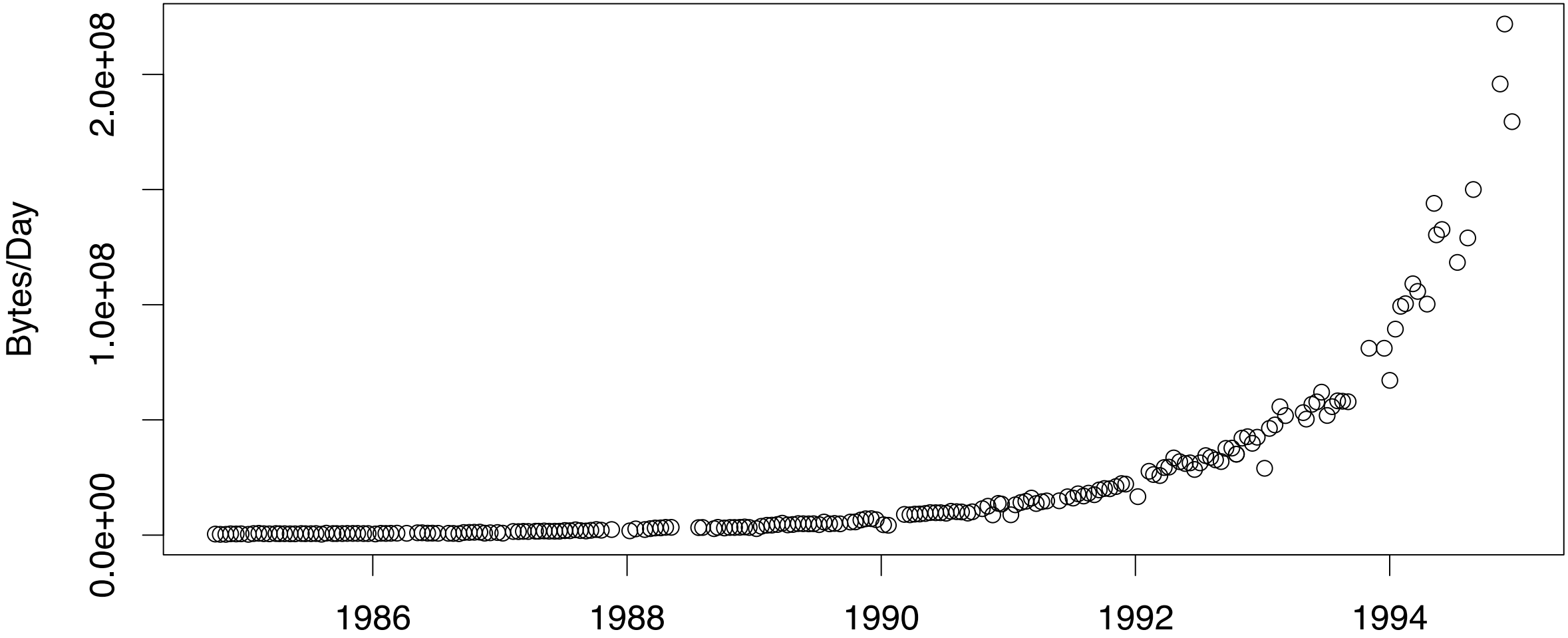
RSAC 2025 Conference

Decade #1 (1984-1996)

Searching for Invariants

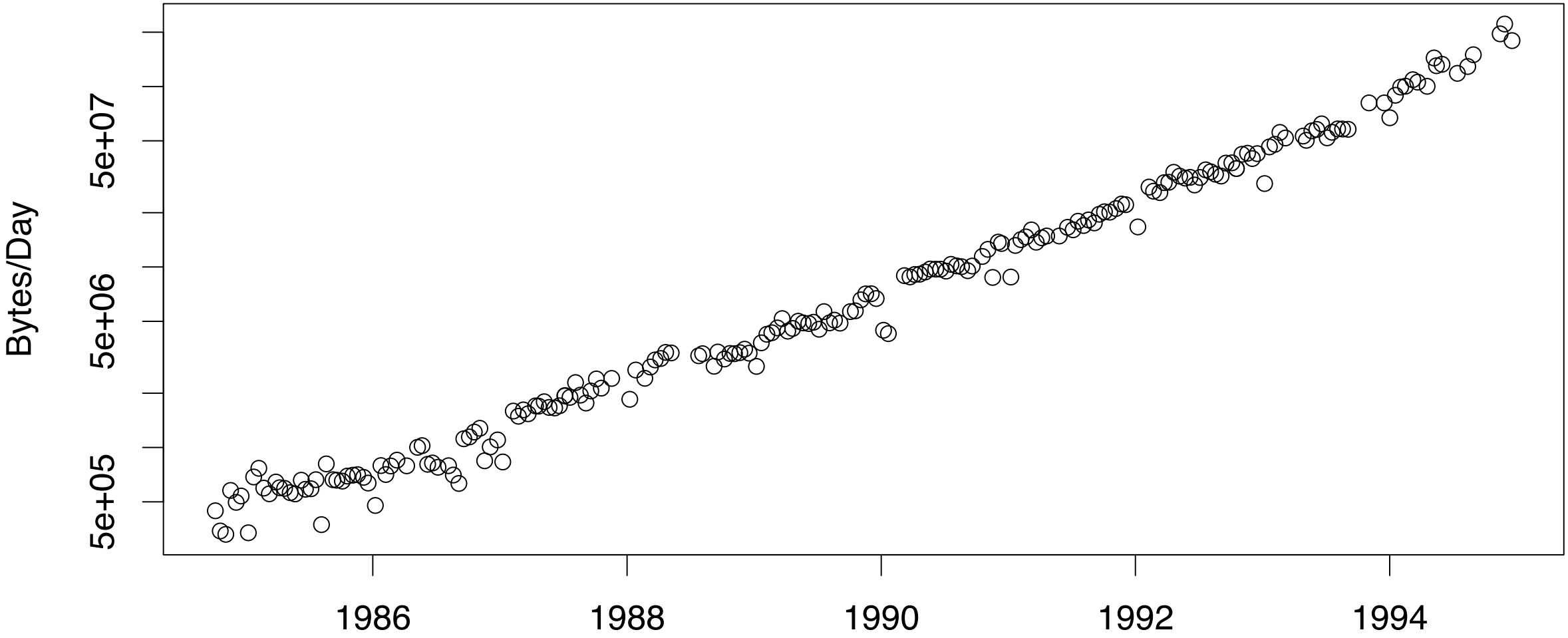
Many Voices.
One Community.

USENET Bulletin Board Traffic Volume



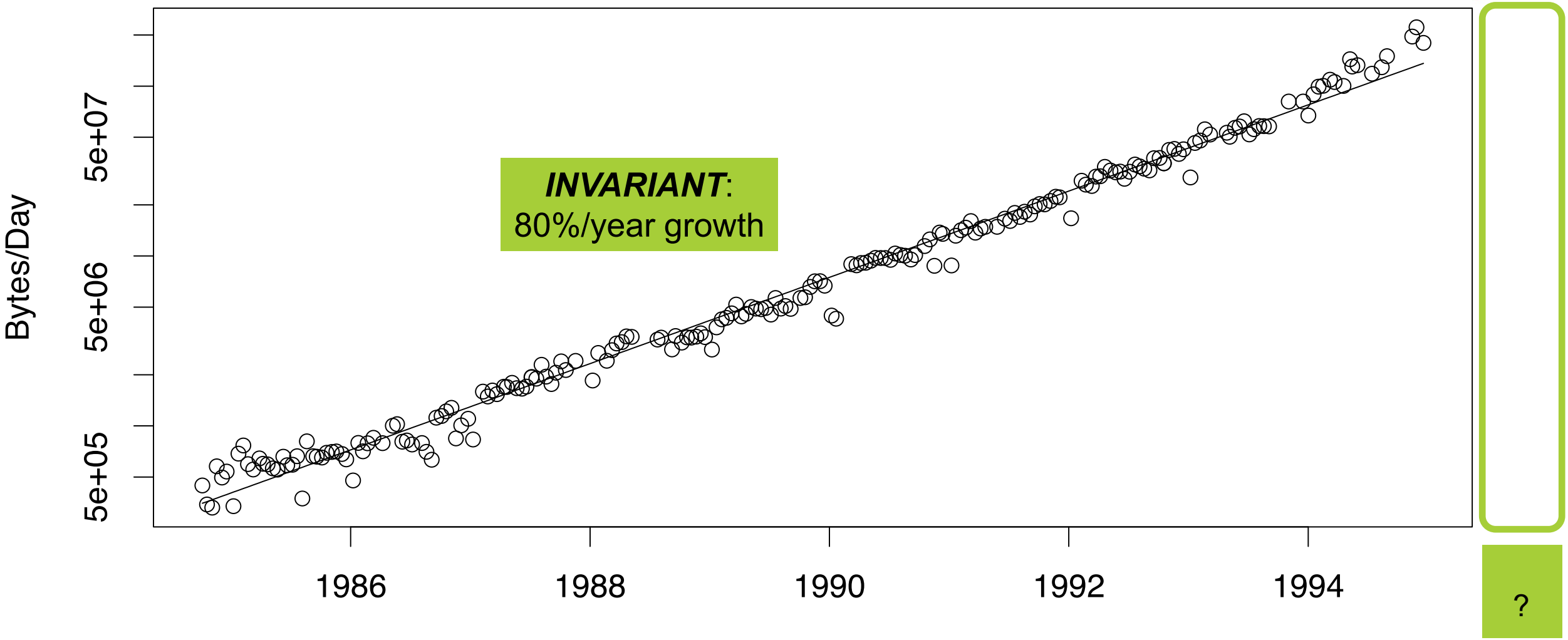
Data courtesy Rick Adams

USENET Bulletin Board Traffic Volume

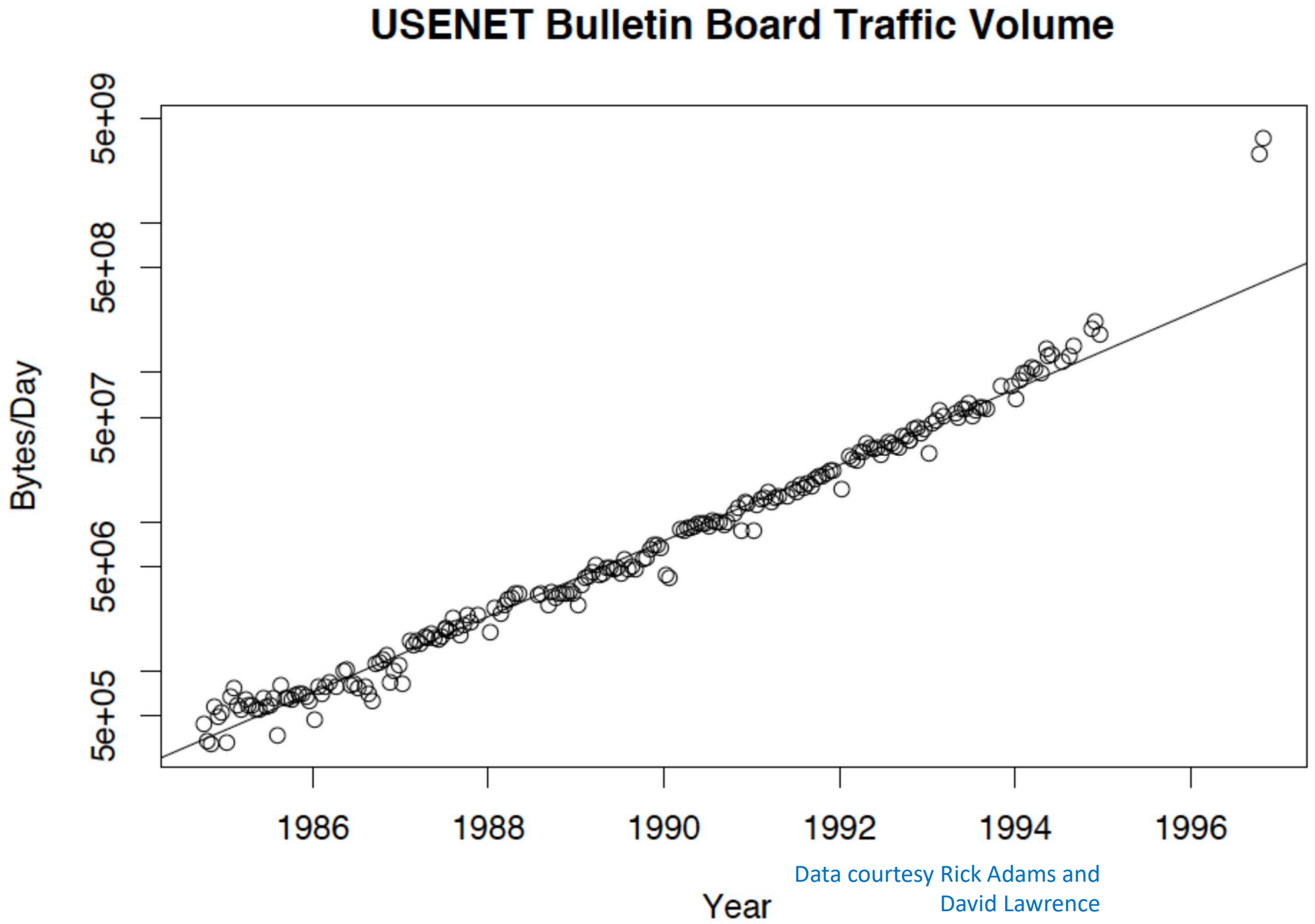


Data courtesy Rick Adams

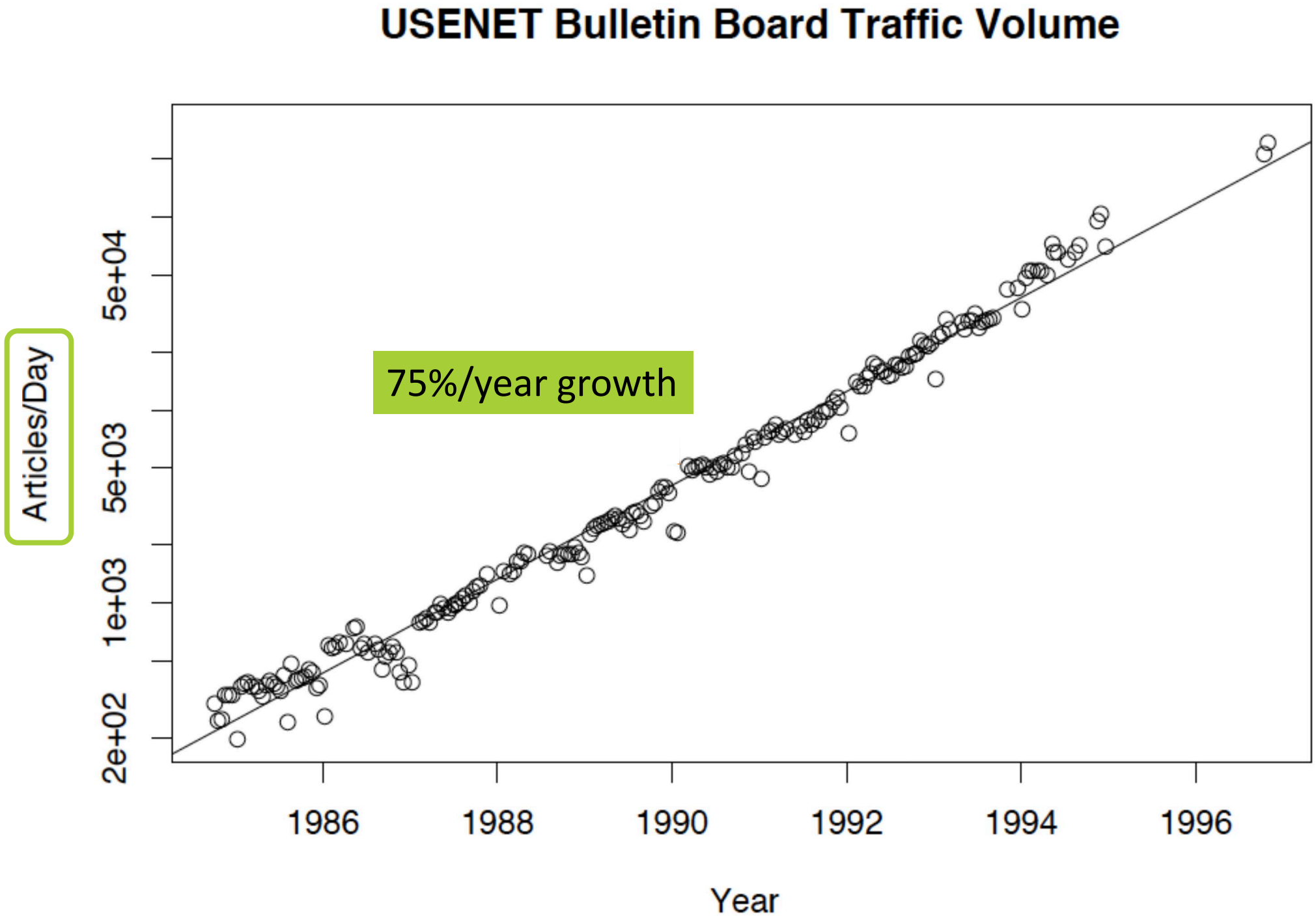
USENET Bulletin Board Traffic Volume

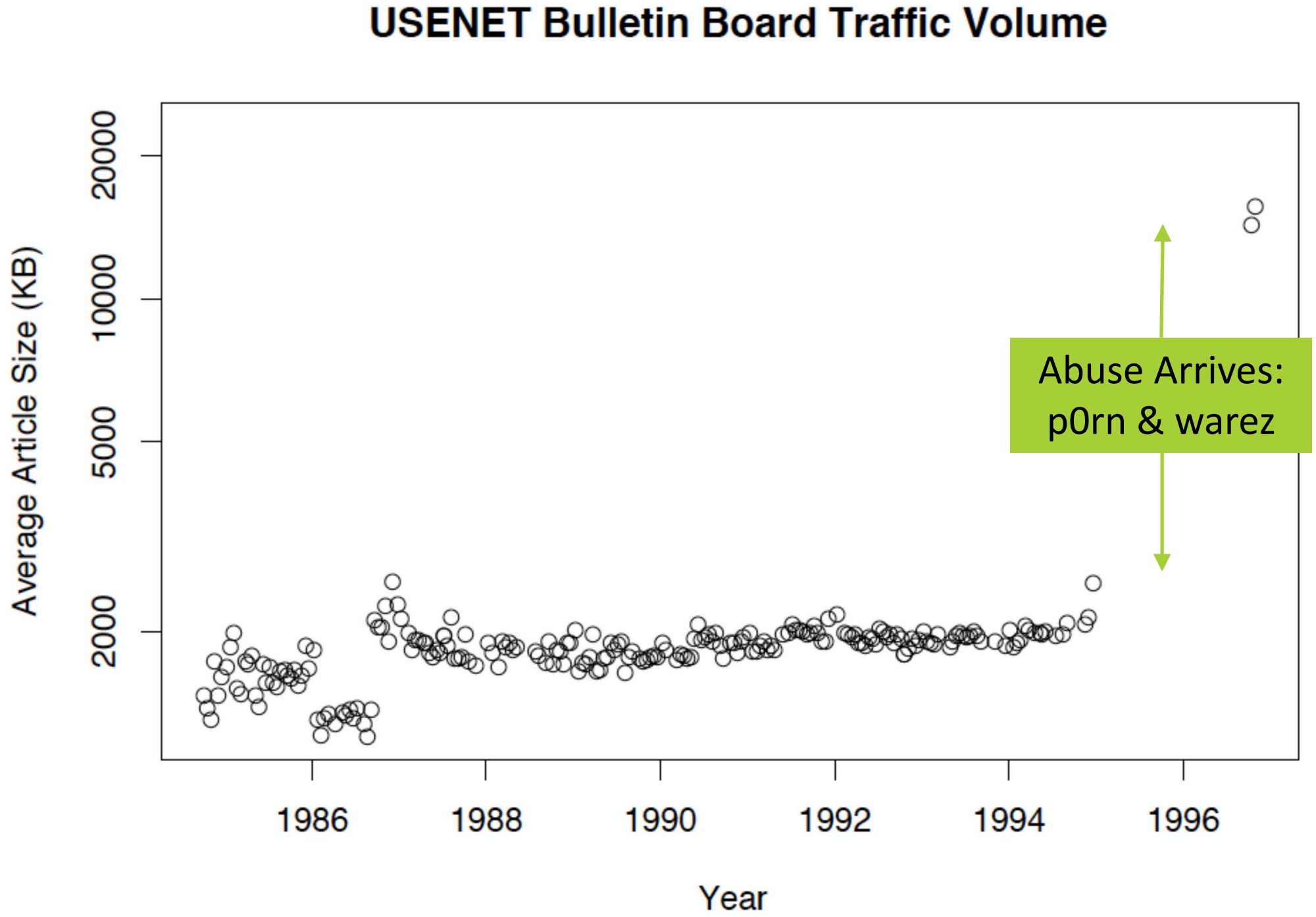


Data courtesy Rick Adams



Data courtesy Rick Adams and David Lawrence


USENET Bulletin Board Traffic Volume
Articles/Day
2e+02
1e+03
5e+03
5e+04
75%/year growth
1986
1988
1990
1992
1994
1996
Year

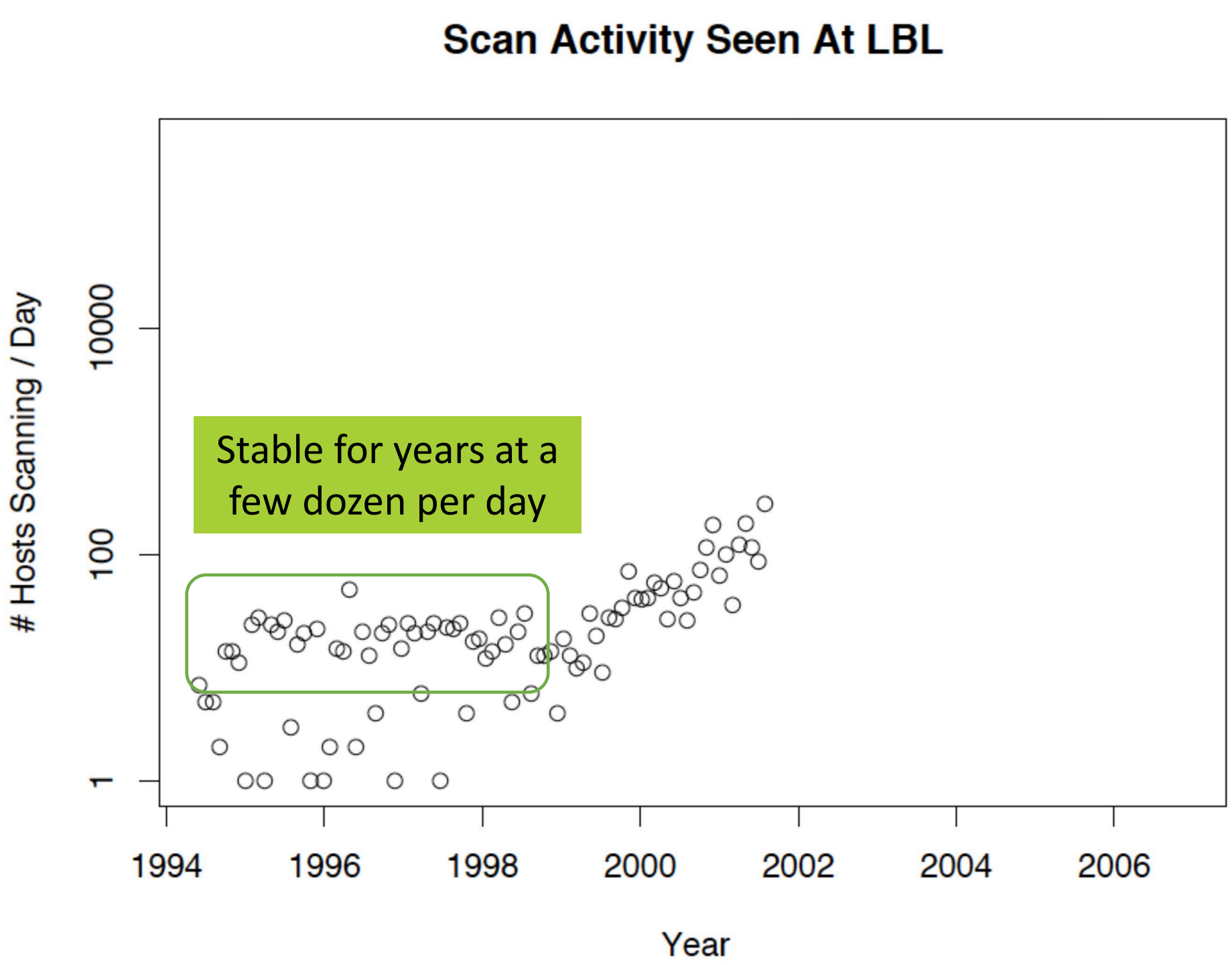

USENET Bulletin Board Traffic Volume
Average Article Size (KB)
2000
5000
10000
20000
1986
1988
1990
1992
1994
1996
Year
Abuse Arrives:
p0rn & warez

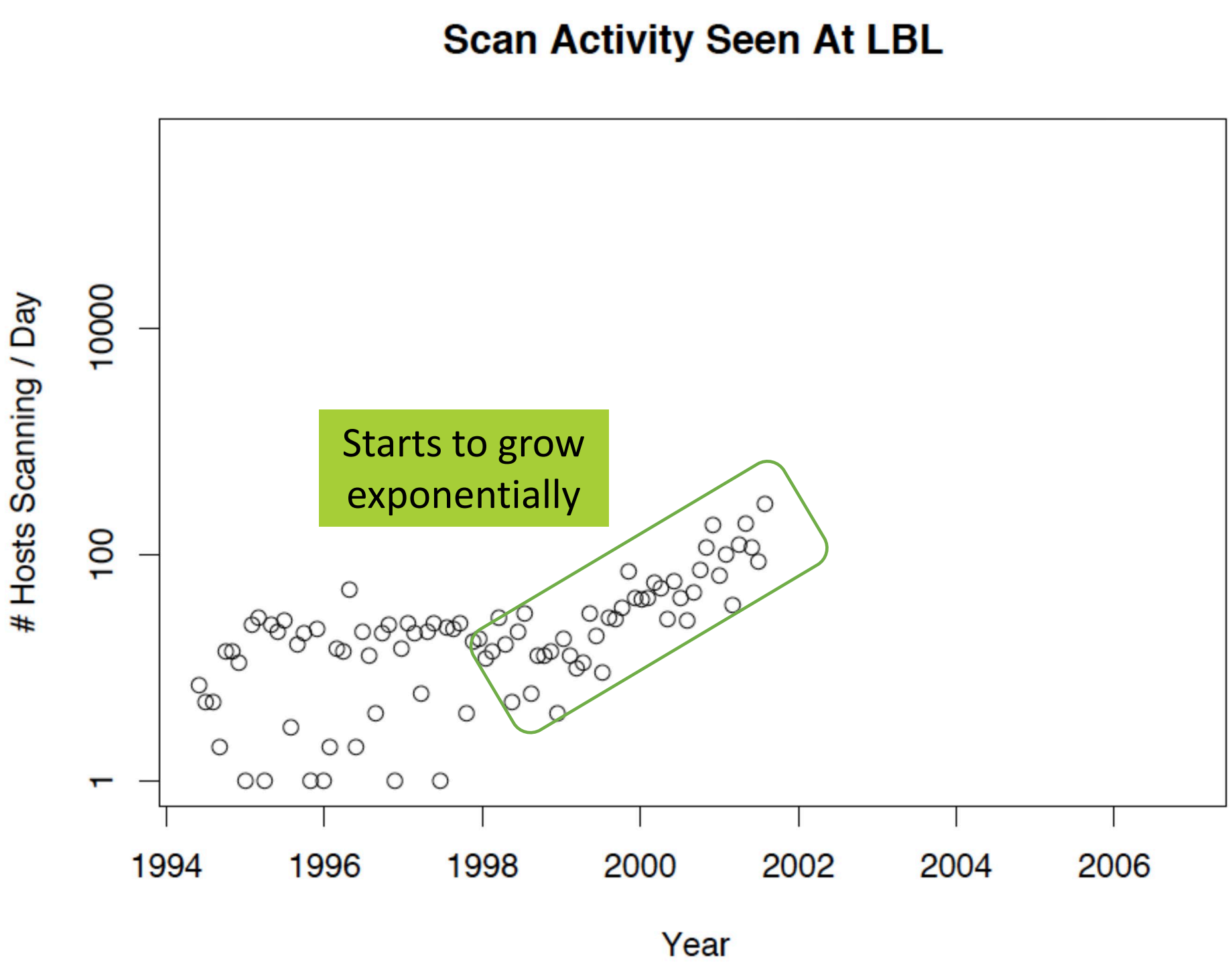
RSAC 2025 Conference

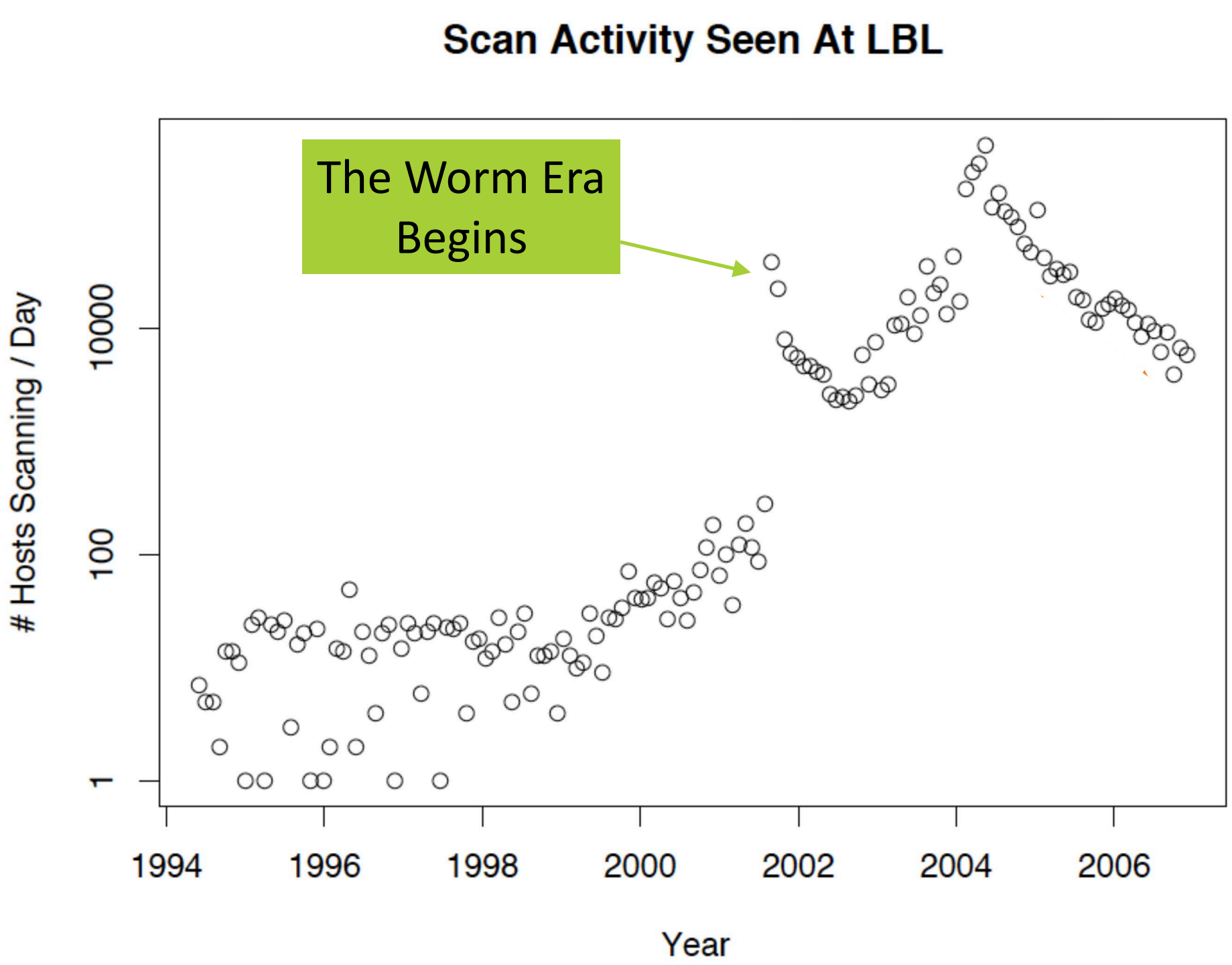
Decade #2 (1994-2006)

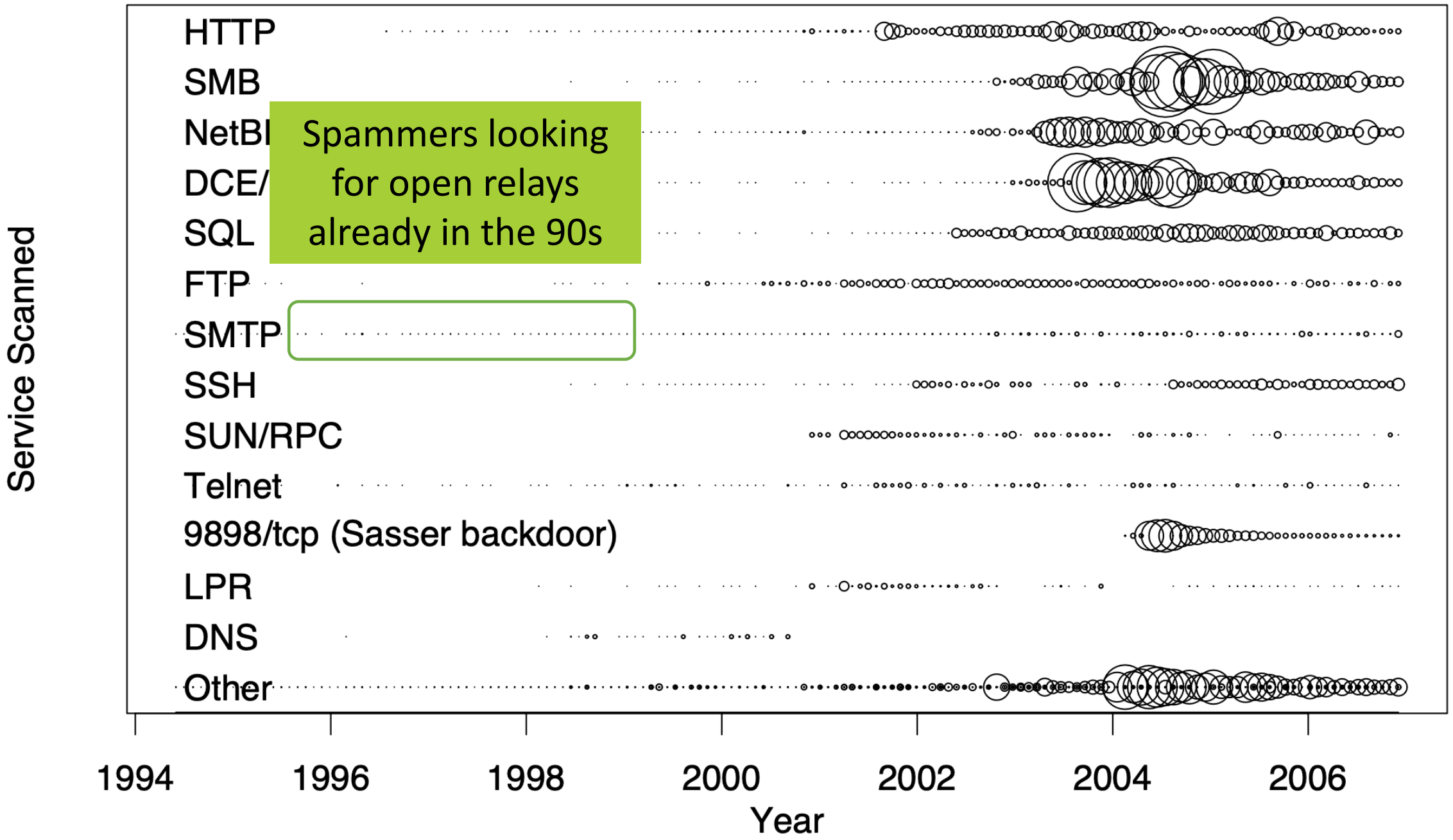
Things Can Change Darn Quickly

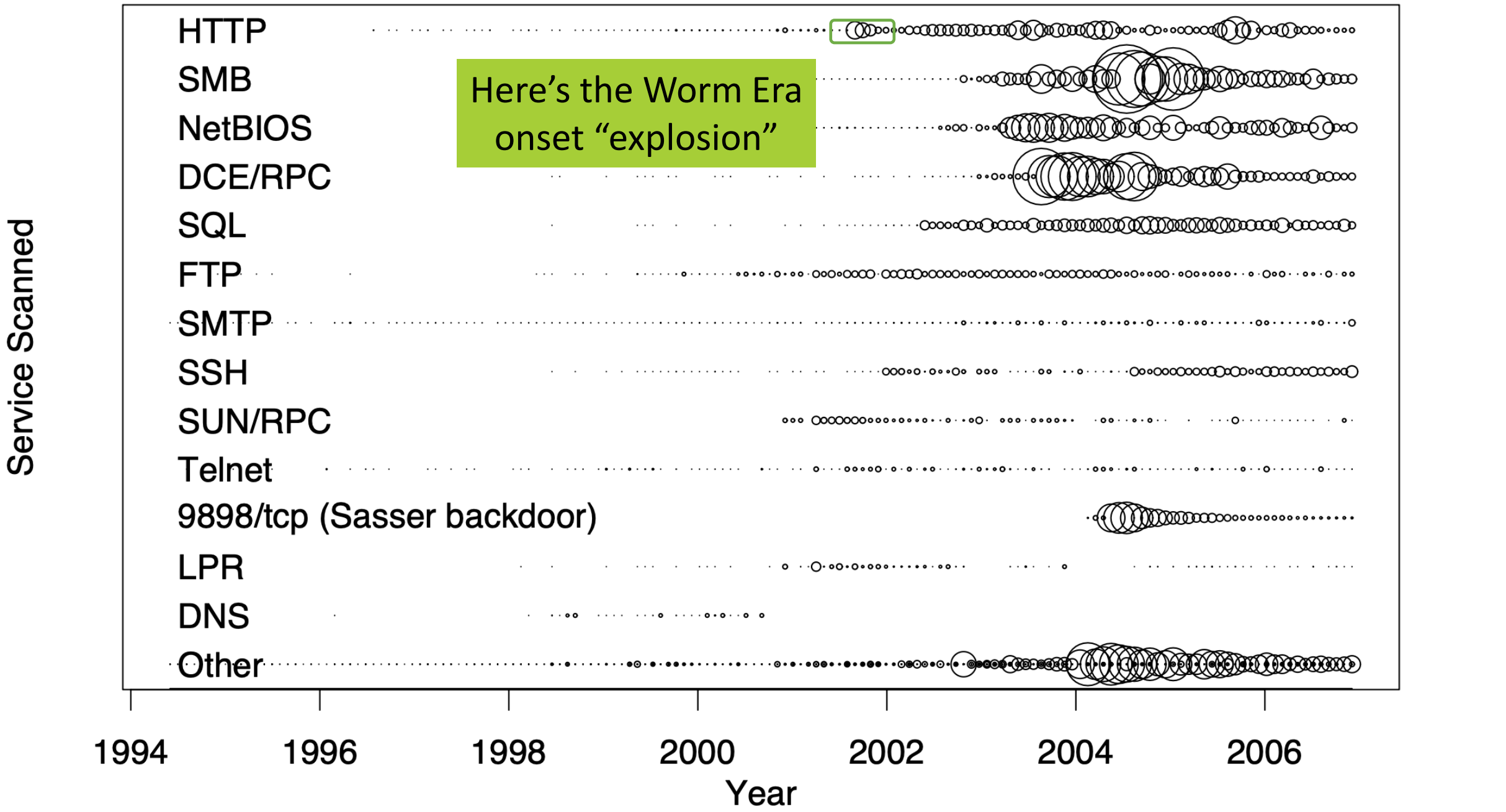
Many Voices.
One Community.

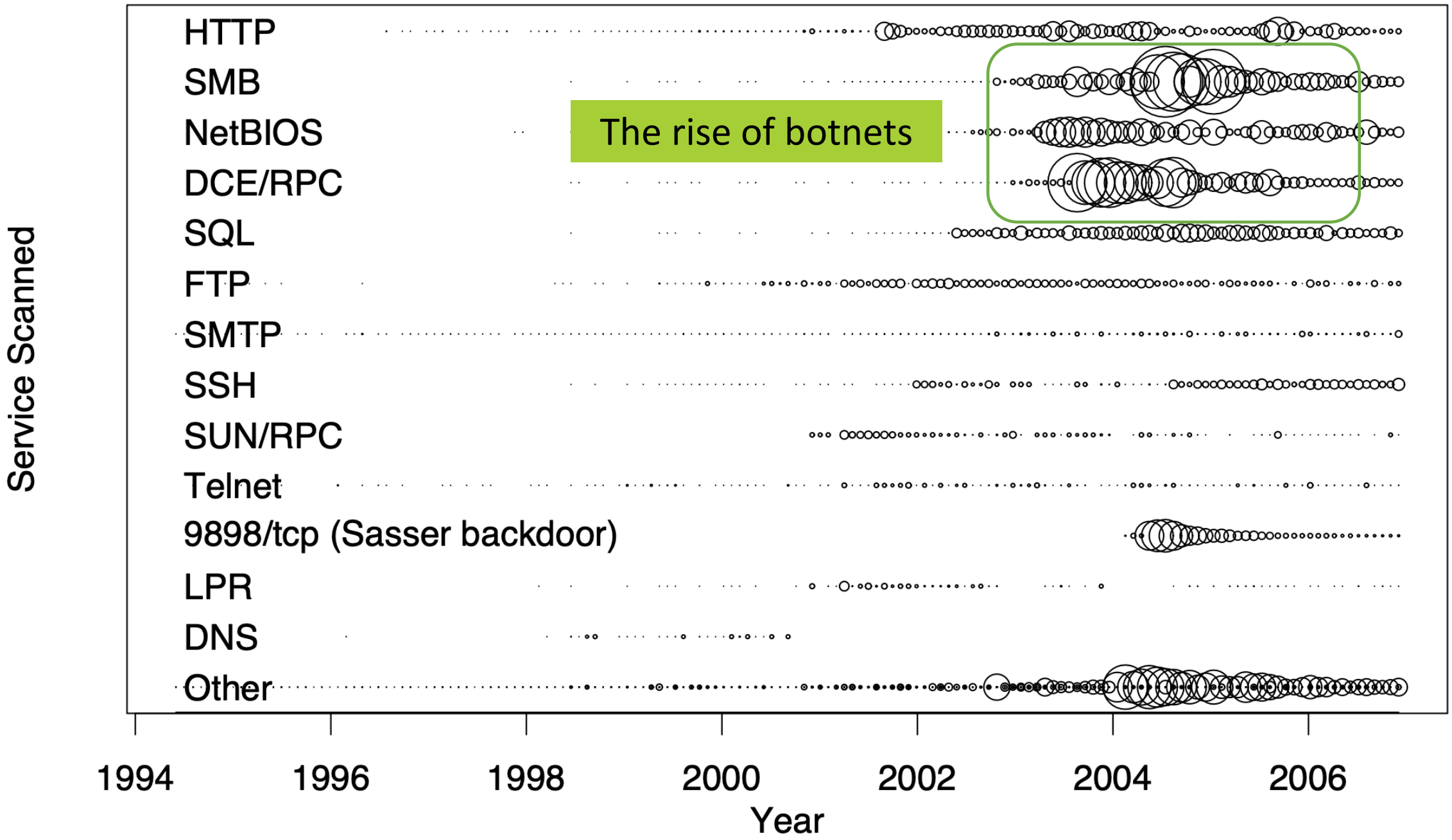

Scan Activity Seen At LBL
Hosts Scanning / Day
10000
100
1
Stable for years at a few dozen per day
1994
1996
1998
2000
2002
2004
2006
Year

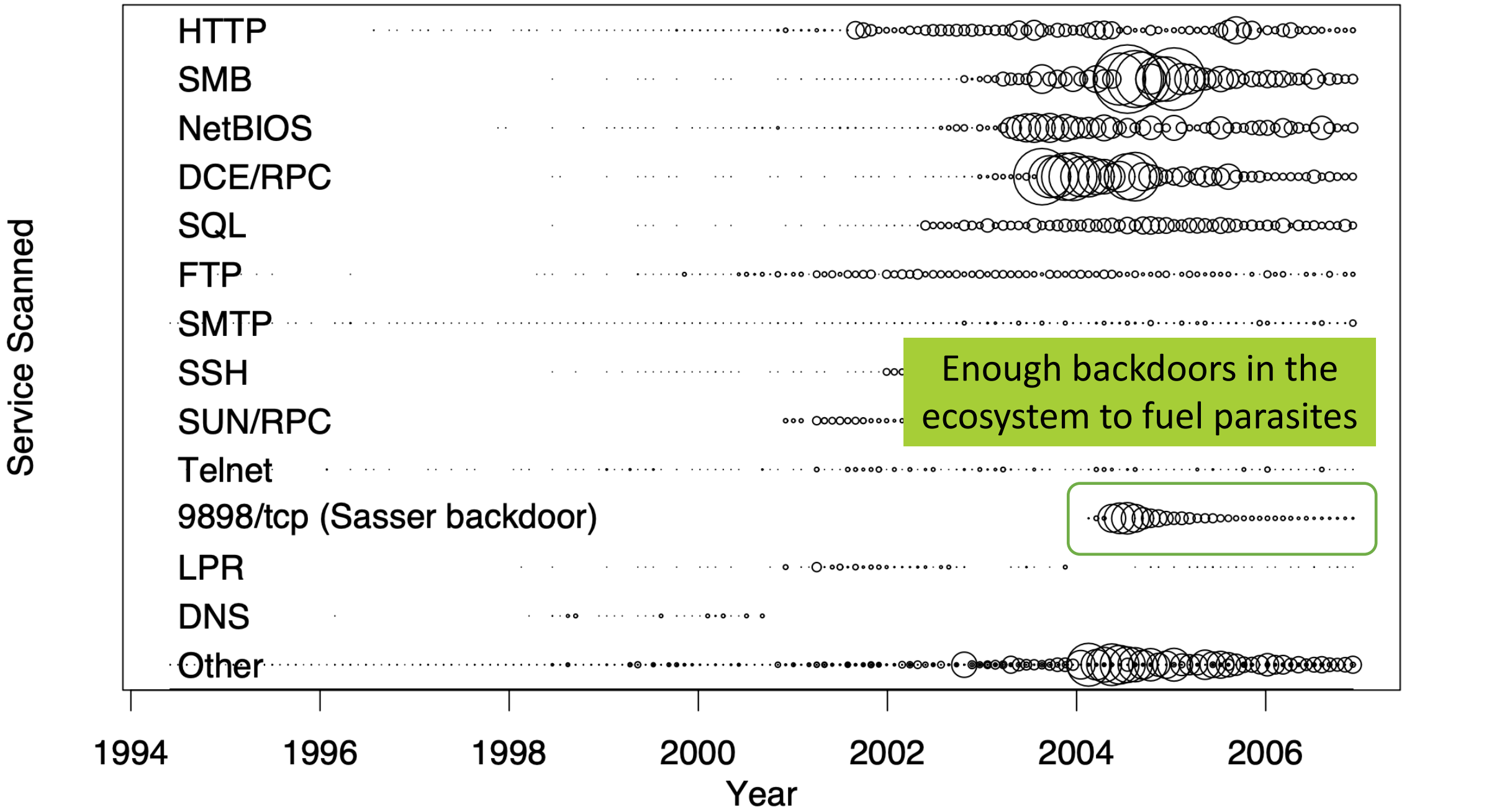

Scan Activity Seen At LBL
Hosts Scanning / Day
10000
100
1
Starts to grow exponentially
1994
1996
1998
2000
2002
2004
2006
Year

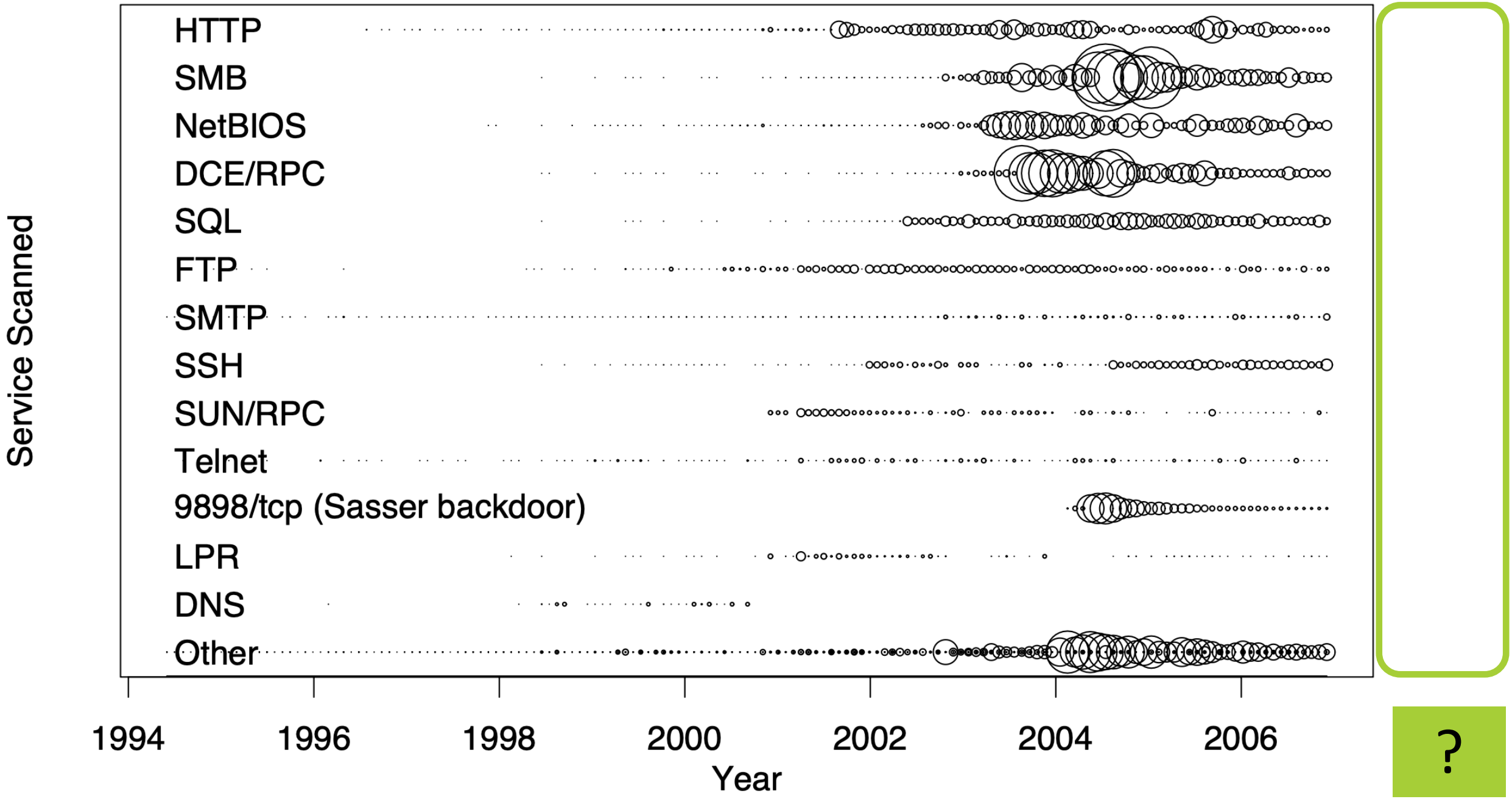

Scan Activity Seen At LBL
The Worm Era Begins
Hosts Scanning / Day
1
100
10000
1994
1996
1998
2000
2002
2004
2006
Year


Service Scanned
HTTP
SMB
NetBI
DCE/
SQL
FTP
SMTP
SSH
SUN/RPC
Telnet
9898/tcp (Sasser backdoor)
LPR
DNS
Other
Spammers looking for open relays already in the 90s
1994
1996
1998
2000
2002
2004
2006
Year


Here's the Worm Era onset "explosion"
Service Scanned
HTTP
SMB
NetBIOS
DCE/RPC
SQL
FTP
SMTP
SSH
SUN/RPC
Telnet
9898/tcp (Sasser backdoor)
LPR
DNS
Other
1994
1996
1998
2000
2002
2004
2006
Year


Service Scanned
HTTP
SMB
NetBIOS
DCE/RPC
SQL
FTP
SMTP
SSH
SUN/RPC
Telnet
9898/tcp (Sasser backdoor)
LPR
DNS
Other
The rise of botnets
1994
1996
1998
2000
2002
2004
2006
Year


Service Scanned
HTTP
SMB
NetBIOS
DCE/RPC
SQL
FTP
SMTP
SSH
SUN/RPC
Telnet
9898/tcp (Sasser backdoor)
LPR
DNS
Other
Enough backdoors in the ecosystem to fuel parasites
1994
1996
1998
2000
2002
2004
2006
Year


Service Scanned
HTTP
SMB
NetBIOS
DCE/RPC
SQL
FTP
SMTP
SSH
SUN/RPC
Telnet
9898/tcp (Sasser backdoor)
LPR
DNS
Other
1994
1996
1998
2000
2002
2004
2006
Year

?

RSAC 2025 Conference

Decade #3+ (2007…)

What Has Happened in the Last 18 Years?

Many Voices.
One Community.

The Zeek Network Security Monitor

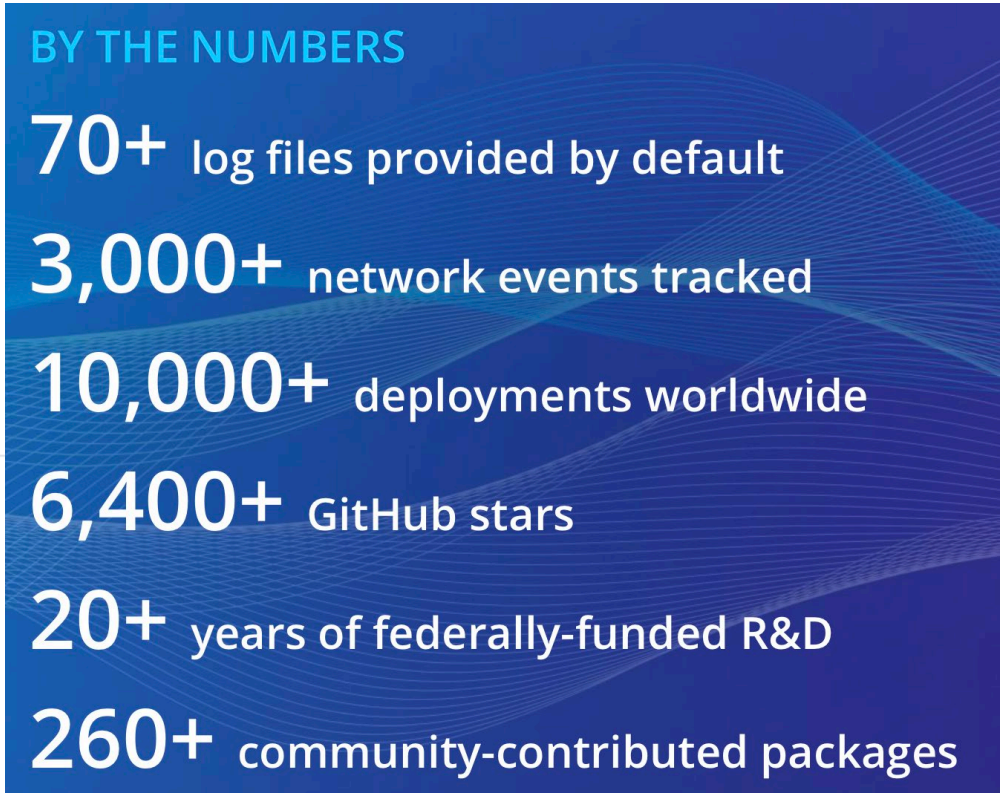
A powerful framework for network traffic analysis and security monitoring.

Key Features — *Documentation* — *Getting Started* — *Development* — *License*

Follow us on Twitter at @zeekurity.

coverage 66% build passing

slack @zeek discourse online



Key Features

- **In-depth Analysis** Zeek ships with analyzers for many protocols, enabling high-level semantic analysis at the application layer.
- **Adaptable and Flexible** Zeek's domain-specific scripting language enables site-specific monitoring policies and means that it is not restricted to any particular detection approach.
- **Efficient** Zeek targets high-performance networks and is used operationally at a variety of large sites.
- **Highly Stateful** Zeek keeps extensive application-layer state about the network it monitors and provides a high-level archive of a network's activity.

Open source since late 1990s

ZEEK® LOGS

conn.log | IP, TCP, UDP, ICMP connection details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of first packet
uid	string	Unique identifier of connection
id	record conn_id	Connection's 4-tuple of endpoints
> id.orig_h	addr	IP address of system initiating connection
> id.orig_p	port	Port from which the connection is initiated
> id.resp_h	addr	IP address of system responding to connection request
> id.resp_p	port	Port on which connection response is sent
proto	enum	Transport layer protocol of connection
service	string	Application protocol ID sent over connection
duration	interval	How long connection lasted
orig_bytes	count	Number of payload bytes originator sent
resp_bytes	count	Number of payload bytes responder sent
conn_state	string	Connection state (see conn.log > conn_state)
local_orig	bool	Value=T if connection originated locally
local_resp	bool	Value=T if connection responded locally
missed_bytes	count	Number of bytes missed (packet loss)
history	string	Connection state history (see conn.log > history)
orig_pkts	count	Number of packets originator sent
orig_ip_bytes	count	Number of originator IP bytes (via IP total_length header field)
resp_pkts	count	Number of packets responder sent
resp_ip_bytes	count	Number of responder IP bytes (via IP total_length header field)
tunnel_parents	table	If tunneled, connection UID value of encapsulating parent(s)
orig_l2_addr	string	Link-layer address of originator
resp_l2_addr	string	Link-layer address of responder
vlan	int	Outer VLAN for connection
inner_vlan	int	Inner VLAN for connection

irc.log | IRC communication details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when command seen
uid & id		Underlying connection info > See conn.log
nick	string	Nickname given for connection
user	string	Username given for connection
command	string	Command given by client
value	string	Value for command given by client
addl	string	Any additional data for command
dcc_file_name	string	DCC filename requested
dcc_file_size	count	DCC transfer size as indicated by sender
dcc_mime_type	string	Sniffed mime type of file
fuid	string	File unique ID

dce_rpc.log | Details on DCE/RPC messages

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened

dhcp.log | DHCP lease activity

FIELD	TYPE	DESCRIPTION
ts	time	Earliest time DHCP message observed
uids	table	Unique Identifiers of DHCP connections
client_addr	addr	IP address of client
server_addr	addr	IP address of server handing out lease
client_port	port	Client port at time of server handing out IP
server_port	port	Server port at time of server handing out IP
mac	string	Client's hardware address
host_name	string	Name given by client in Hostname option 12
client_fqdn	string	FQDN given by client in Client FQDN option 81
domain	string	Domain given by server in option 15
requested_addr	addr	IP address requested by client
assigned_addr	addr	IP address assigned by server
lease_time	interval	IP address lease interval
client_message	string	Message with DHCP_DECLINE so client can tell server why address was rejected
server_message	string	Message with DHCP_NAK to let client know why request was rejected
msg_types	vector	DHCP message types seen by transaction
duration	interval	Duration of DHCP session
client_chaddr	string	Hardware address reported by the client
msg_orig	vector	Address originated from msg_types field
client_software	string	Software reported by client in vendor_class
server_software	string	Software reported by server in vendor_class
circuit_id	string	DHCP relay agents that terminate circuits
agent_remote_id	string	Globally unique ID added by relay agents to identify remote host end of circuit
subscriber_id	string	Value independent of physical network connection that provides customer DHCP configuration regardless of physical location

kerberos.log | Kerberos authentication

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid & id		Underlying connection info > See conn.log
request_type	string	Authentication Service (AS) or Ticket Granting Service (TGS)
client	string	Client
service	string	Service
success	bool	Request result
error_msg	string	Error message
from	time	Ticket valid from
till	time	Ticket valid until
cipher	string	Ticket encryption type
forwardable	bool	Forwardable ticket requested
renewable	bool	Renewable ticket requested
client_cert_subject	string	Subject of client certificate, if any
client_cert_fuid	string	File unique ID of client cert, if any
server_cert_subject	string	Subject of server certificate, if any
server_cert_fuid	string	File unique ID of server cert, if any
auth_ticket	string	Ticket hash authorizing request/transaction
new_ticket	string	Ticket hash returned by KDC

dns.log | DNS query/response details

FIELD	TYPE	DESCRIPTION
ts	time	Earliest timestamp of DNS protocol message
uid & id		Underlying connection info > See conn.log
proto	enum	Transport layer protocol of connection
trans_id	count	16-bit identifier assigned by program that generated DNS query
rtt	interval	Round trip time for query and response
query	string	Domain name subject of DNS query
qclass	count	QCLASS value specifying query class
qclass_name	string	Descriptive name query class
qtype	count	QTYPE value specifying query type
qtype_name	string	Descriptive name for query type
rcode	count	Response code value in DNS response
rcode_name	string	Descriptive name of response code value
AA	bool	Authoritative Answer bit: responding name server is authority for domain name
TC	bool	Truncation bit: message was truncated
RD	bool	Recursion Desired bit: client wants recursive service for query
RA	bool	Recursion Available bit: name server supports recursive queries
Z	count	Reserved field, usually zero in queries and responses
answers	vector	Set of resource descriptions in query answer
TTLs	vector	Caching intervals of RRs in answers field
rejected	bool	DNS query was rejected by server
auth	table	Authoritative responses for query
addl	table	Additional responses for query

dpd.log | Dynamic protocol detection failures

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when protocol analysis failed
uid & id		Underlying connection info > See conn.log
proto	enum	Transport protocol for violation
analyzer	string	Analyzer that generated violation
failure_reason	string	Textual reason for analysis failure
packet_segment	string	Payload chunk that most likely resulted in protocol violation

modbus.log | PLC requests (ICS)

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the PLC request
uid & id		Underlying connection info > See conn.log

mysql.log | MySQL

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid & id		Underlying connection info > See conn.log
cmd	string	Command that was issued
arg	string	Argument issued to command
success	bool	Server replied command succeeded
rows	count	Number of affected rows, if any
response	string	Server message, if any

files.log | File analysis results

FIELD	TYPE	DESCRIPTION
ts	time	Time when file first seen
fuid	string	Identifier associated with single file
uid & id		Underlying connection info > See conn.log
source	string	Identification of file data source
depth	count	Value to represent depth of file in relation to source
analyzers	table	Set of analysis types done during file analysis
mime_type	string	Mime type, as determined by Zeek's signatures
filename	string	Filename, if available from file source
duration	interval	Duration file was analyzed for
local_orig	bool	Indicates if data originated from local network
is_orig	bool	If file sent by connection originator or responder
seen_bytes	count	Number of bytes provided to file analysis engine
total_bytes	count	Total number of bytes that should comprise full file
missing_bytes	count	Number of bytes in file stream missed
overflow_bytes	count	Number of bytes in file stream not delivered to stream file analyzers
timedout	bool	If file analysis timed out at least once
parent_fuid	string	Container file ID was extracted from
md5	string	MD5 digest of file contents
sha1	string	SHA1 digest of file contents
sha256	string	SHA256 digest of file contents
extracted	string	Local filename of extracted file
extracted_cutoff	bool	Set to true if file being extracted was cut off so whole file was not logged
extracted_size	count	Number of bytes extracted to disk
entropy	double	Information density of file contents

pe.log | Portable executable

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
id	string	File id of this portable executable file
machine	string	Target machine file was compiled for
compile_ts	time	Time file was created
os	string	Required operating system
subsystem	string	Subsystem required to run this file
is_exe	bool	Is file an executable, or just an object file?
is_64bit	bool	Is file a 64-bit executable?
uses_aslr	bool	Does file support Address Space Layout Randomization?
uses_dep	bool	Does file support Data Execution Prevention?
uses_code_integrity	bool	Does file enforce code integrity checks?
uses_seh	bool	Does file use structured exception handing?
has_import_table	bool	Does file have import table?
has_export_table	bool	Does file have export table?
has_cert_table	bool	Does file have attribute certificate table?
has_debug_data	bool	Does file have debug table?
section_names	vector of string	Names of sections, in order

ftp.log | FTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when command sent
uid & id		Underlying connection info > See conn.log
user	string	Username for current FTP session
password	string	Password for current FTP session
command	string	Command given by client
arg	string	Argument for command, if given
mime_type	string	Sniffed mime type of file
file_size	count	Size of file
reply_code	count	Reply code from server in response to command
reply_msg	string	Reply code from server in response to command
data_channel	record FTP::: Expected Data Channel	Expected FTP data channel
fuid	string	File unique ID

http.log | HTTP request/reply details

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when request happened
uid & id		Underlying connection info > See conn.log
trans_depth	count	Pipelined depth into connection
method	string	Verb used in HTTP request (GET, POST, etc.)
host	string	Value of HOST header
uri	string	URI used in request
referrer	string	Value of referer header
version	string	Value of version portion of request
user_agent	string	Value of User-Agent header from client
origin	string	Value of Origin header from client
request_body_len	count	Uncompressed data size from client
response_body_len	count	Uncompressed data size from server
status_code	count	Status code returned by server
status_msg	string	Status message returned by server
info_code	count	Last seen 1xx info reply code from server
info_msg	string	Last seen 1xx info reply message from server
tags	table	Indicators of various attributes discovered
username	string	Username if basic-auth performed for request
password	string	Password if basic-auth performed for request
proxied	table	All headers indicative of proxied request
orig_fuids	vector	Ordered vector of file unique IDs
orig_filenames	vector	Ordered vector of filenames from client
orig_mime_types	vector	Ordered vector of mime types
resp_fuids	vector	Ordered vector of file unique IDs
resp_filenames	vector	Ordered vector of filenames from server
resp_mime_types	vector	Ordered vector of mime types

corelight

ZEEK® LOGS

radius.log | RADIUS authentication attempts

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp for when event happened
uid & id		Underlying connection info > See conn.log
username	string	Username, if present
mac	string	MAC address, if present
framed_addr	addr	Address given to network access server, if present
tunnel_client	string	Address (IPv4, IPv6, or FQDN) of initiator end of tunnel, if present
connect_info	string	Connect info, if present
reply_msg	string	Reply message from server challenge
result	string	Successful or failed authentication
ttl	interval	Duration between first request and either Access-Accept message or an error

sip.log | SIP analysis

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when request happened
uid & id		Underlying connection info > See conn.log
trans_depth	count	Pipelined depth into request/response transaction
method	string	Verb used in SIP request (INVITE, etc)
uri	string	URI used in request
date	string	Contents of Date: header from client
request_from	string	Contents of request From: header[1]
request_to	string	Contents of To: header
response_from	string	Contents of response From: header[1]
response_to	string	Contents of response To: header
reply_to	string	Contents of Reply-To: header
call_id	string	Contents of Call-ID: header from client
seq	string	Contents of CSeq: header from client
subject	string	Contents of Subject: header from client
request_path	vector	Client message transmission path, extracted from headers
response_path	vector	Server message transmission path, extracted from headers
user_agent	string	Contents of User-Agent: header from client
status_code	count	Status code returned by server
status_msg	string	Status message returned by server
warning	string	Contents of Warning: header
request_body_len	count	Contents of Content-Length: header from client
response_body_len	count	Contents of Content-Length: header from server
content_type	string	Contents of Content-Type: header from server

tunnel.log | Details of encapsulating tunnels

FIELD	TYPE	DESCRIPTION
ts	time	Time at which tunnel activity occurred

smb_mapping.log | SMB mappings

FIELD	TYPE	DESCRIPTION
ts	time	Time when tree was mapped
uid & id		Underlying connection info > See conn.log
path	string	Name of tree path
service	string	Type of resource of tree (disk share, printer share, named pipe, etc)
native_file_system	string	File system of tree
share_type	string	If this is SMB2, share type will be included

smtp.log | SMTP transactions

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when message was first seen
uid & id		Underlying connection info > See conn.log
trans_depth	count	Transaction depth if there are multiple msgs
helo	string	Contents of Helo header
mailfrom	string	Email addresses found in From header
rcptto	table	Email addresses found in Rcpt header
date	string	Contents of Date header
from	string	Contents of From header
to	table	Contents of To header
cc	table	Contents of CC header
reply_to	string	Contents of ReplyTo header
msg_id	string	Contents of MsgID header
in_reply_to	string	Contents of In-Reply-To header
subject	string	Contents of Subject header
x_originating_ip	addr	Contents of X-Originating-IP header
first_received	string	Contents of first Received header
second_received	string	Contents of second Received header
last_reply	string	Last message server sent to client
path	vector	Message transmission path, from headers
user_agent	string	Value of User-Agent header from client
tls	bool	Indicates connection switched to using TLS
fuids	vector	File unique IDs attached to message
is_webmail	bool	If message sent via webmail

snmp.log | SNMP messages

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of first packet of SNMP session
uid & id		Underlying connection info > See conn.log
duration	interval	Amount of time between first packet belonging to SNMP session and latest seen
version	string	Version of SNMP being used
community	string	Community string of first SNMP packet associated with session
get_requests	count	Number of variable bindings in GetRequest/GetNextRequest PDUs seen for session
get_bulk_requests	count	Number of variable bindings in GetBulkRequest PDUs seen for session
get_responses	count	Number of variable bindings in GetResponse/Response PDUs seen for session
set_requests	count	Number of variable bindings in SetRequest PDUs seen for session
display_string	string	System description of SNMP responder endpoint
up_since	time	Time at which SNMP responder endpoint claims it's been up since

socks.log | SOCKS proxy requests

FIELD	TYPE	DESCRIPTION
ts	time	Time when proxy connection detected
uid & id		Underlying connection info > See conn.log
version	count	Protocol version of SOCKS
user	string	Username used to request a login to proxy
password	string	Password used to request a login to proxy
status	string	Server status for attempt at using proxy
request	record SOCKS::Address	Client requested SOCKS address
request_p	port	Client requested port
bound	record SOCKS::Address	Server bound address
bound_p	port	Server bound port

software.log | Software observed on network

FIELD	TYPE	DESCRIPTION
ts	time	Time at which software was detected
host	addr	IP address detected running the software
host_p	port	Port on which software is running
software_type	enum	Type of software detected (e.g., HTTP::SERVER)
name	string	Name of software (e.g., Apache)
version	record Software::Version	Software version
unparsed_version	string	Full, unparsed version string found
url	string	Root URL where software was discovered

ssh.log | SSH handshakes

FIELD	TYPE	DESCRIPTION
ts	time	Time when SSH connection began
uid & id		Underlying connection info > See conn.log
version	count	SSH major version (1 or 2)
auth_success	bool	Authentication result (T=success, F=failure, unset=unknown)
auth_attempts	count	Number of authentication attempts observed
direction	enum	Direction of connection
client	string	Client's version string
server	string	Server's version string
cipher_alg	string	Encryption algorithm in use
mac_alg	string	Signing (MAC) algorithm in use
compression_alg	string	Compression algorithm in use
kex_alg	string	Key exchange algorithm in use
host_key_alg	string	Server host key's algorithm
host_key	string	Server's key fingerprint
remote_location	record geo_location	Add geographic data related to remote host of connection

dnp3.log | Distributed Network Protocol (ICS)

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp of the DNP3 request
uid & id		Underlying connection info > See conn.log

ssl.log | SSL handshakes

FIELD	TYPE	DESCRIPTION
ts	time	Time when SSL connection first detected
uid & id		Underlying connection info > See conn.log
version	string	SSL/TLS version server chose
cipher	string	SSL/TLS cipher suite server chose
curve	string	Elliptic curve server chose when using ECDH/ECDHE
server_name	string	Value of Server Name Indicator SSL/TLS extension
resumed	bool	Flag that indicates session was resumed
last_alert	string	Last alert seen during connection
next_protocol	string	Next protocol server chose using application layer next protocol extension, if present
established	bool	Flags if SSL session successfully established
ssl_history	string	SSL history showing which types of packets were received in which order. Client-side letters are capitalized, server-side lower-case
cert_chain_fps	vector	All fingerprints for the certificates offered by the server
client_cert_chain_fps	vector	All fingerprints for the certificates offered by the client
subject	string	Subject of X.509 cert offered by server
issuer	string	Subject of signer of X.509 server cert
client_subject	string	Subject of X.509 cert offered by client
client_issuer	string	Subject of signer of client cert
sni_matches_cert	bool	Set to true if the hostname sent in the SNI matches the certificate, false if they do not. Unset if the client did not send an SNI
request_client_certificate_authorities	vector	List of client certificate CAs accepted by the server
server_version	count	Numeric version of the server in the server hello
client_version	count	Numeric version of the client in the client hello
client_ciphers	vector	Ciphers that were offered by the client for the connection
ssl_client_exts	vector	SSL client extensions
ssl_server_exts	vector	SSL server extensions
ticket_lifetime_hint	count	Suggested ticket lifetime sent in the session ticket handshake by the server
dh_param_size	count	The diffie helman parameter size, when using DH
point_formats	vector	Supported elliptic curve point formats
client_curves	vector	The curves supported by the client
orig_alpn	vector	Application layer protocol negotiation extension sent by the client
client_supported_versions	vector	TLS 1.3 supported versions
server_supported_version	count	TLS 1.3 supported version
psk_key_exchange_modes	vector	TLS 1.3 Pre-shared key exchange modes
client_key_share_groups	vector	Key share groups from client hello
server_key_share_group	count	Selected key share group from server hello

syslog.log | Syslog messages

FIELD	TYPE	DESCRIPTION
ts	time	Timestamp when syslog message was seen
uid & id		Underlying connection info > See conn.log
proto	enum	Protocol over which message was seen
facility	string	Syslog facility for message
severity	string	Syslog severity for message
message	string	Plain text message

smb_files.log | Details on SMB files

FIELD	TYPE	DESCRIPTION
ts	time	Time when file was first discovered
uid & id		Underlying connection info > See conn.log
fuid	string	Unique ID of file
action	enum	Action this log record represents
path	string	Path pulled from tree that file was transferred to or from
name	string	Filename if one was seen
size	count	Total size of file
prev_name	string	If rename action was seen, this will be file's previous name
times	record SMB::MAC-Times	Last time file was modified

weird.log | Unexpected network/protocol

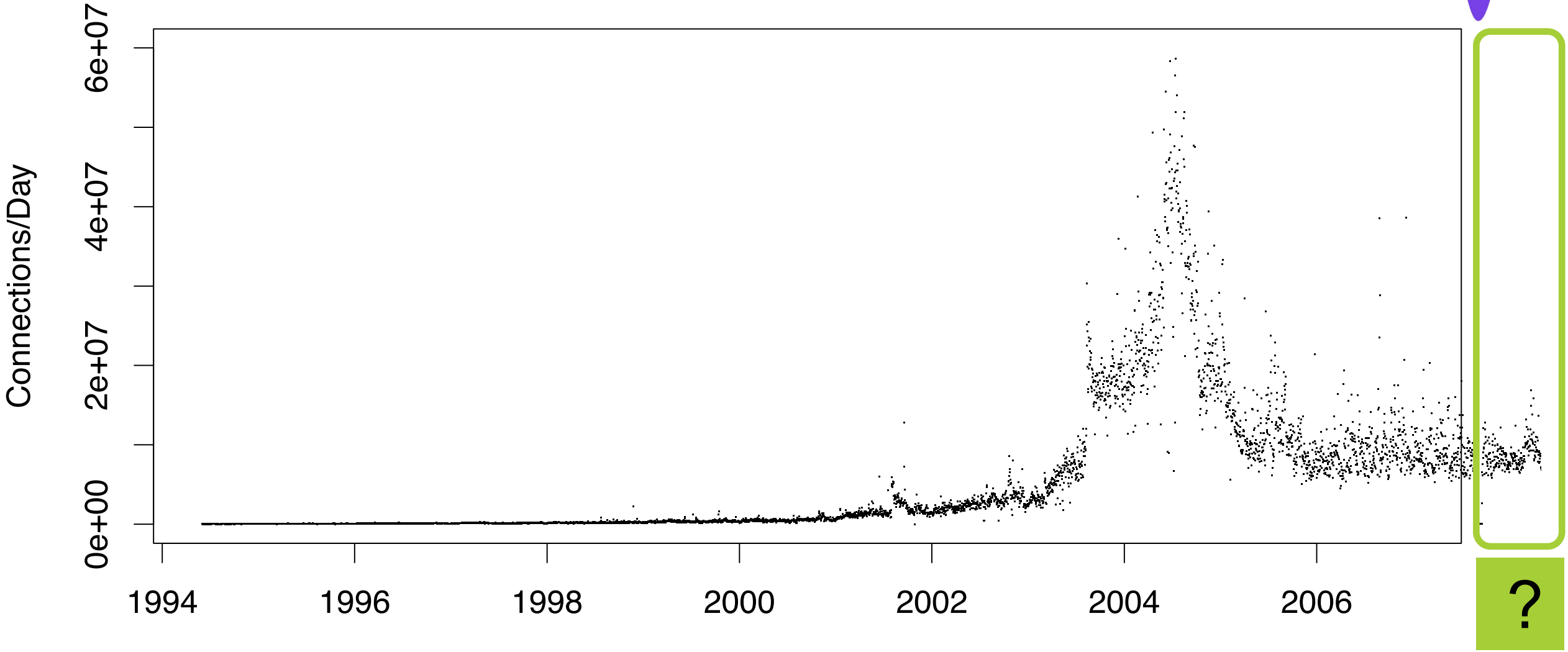
FIELD	TYPE	DESCRIPTION
ts	time	Time when weird occurred
uid & id		Underlying connection info > See conn.log
name	string	Name of weird that occurred
addl	string	Additional information accompanying weird, if any
notice	bool	If weird was turned into a notice
peer	string	Peer that originated weird

x509.log | X.509 certificate info

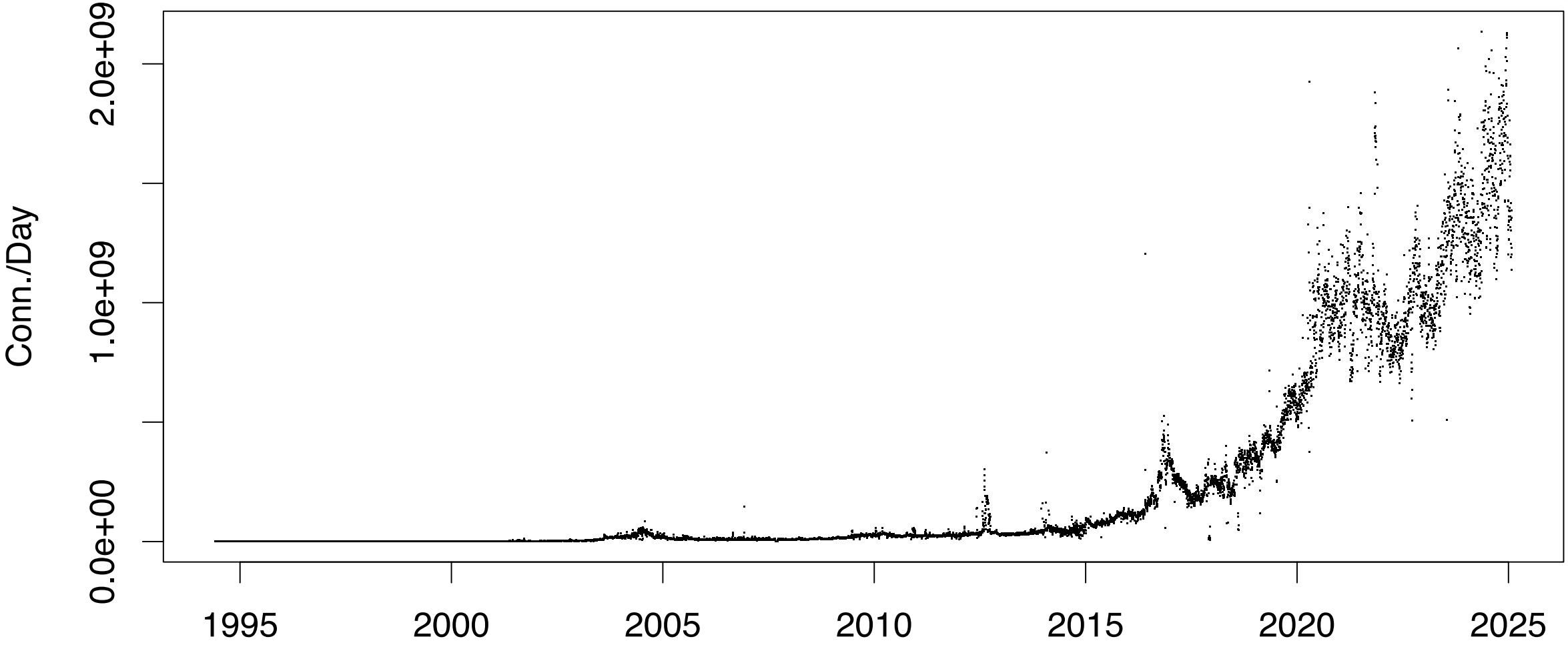
FIELD	TYPE	DESCRIPTION
ts	time	Current timestamp
fingerprint	string	Fingerprint of the certificate
certificate	record X509::Certificate	Basic information about certificate
san	record X509::Subject Alternative Name	Subject alternative name extension of certificate
basic_constraints	record X509::Basic Constraints	Basic constraints extension of certificate

corelight

Evolution of Connections/Day (LBNL)

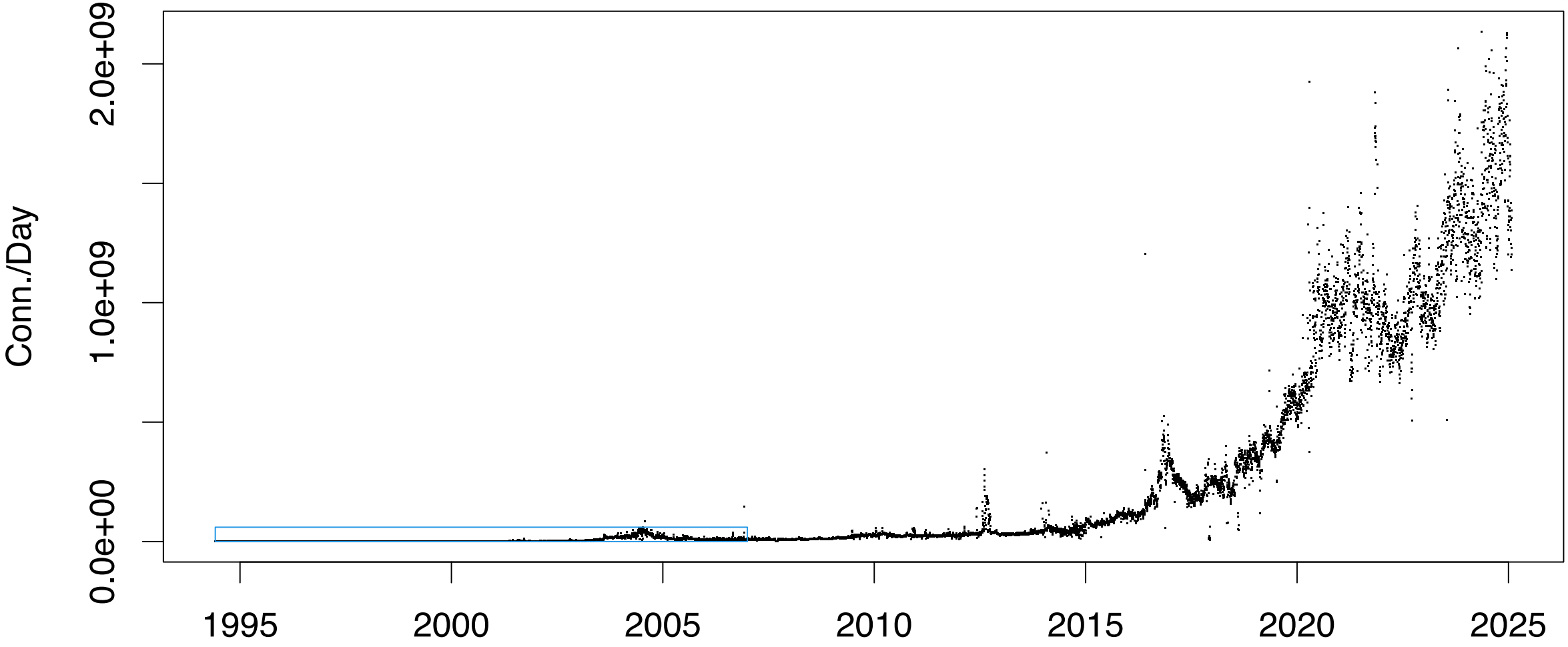


Evolution of Inbound Connections Per Day (LBNL)



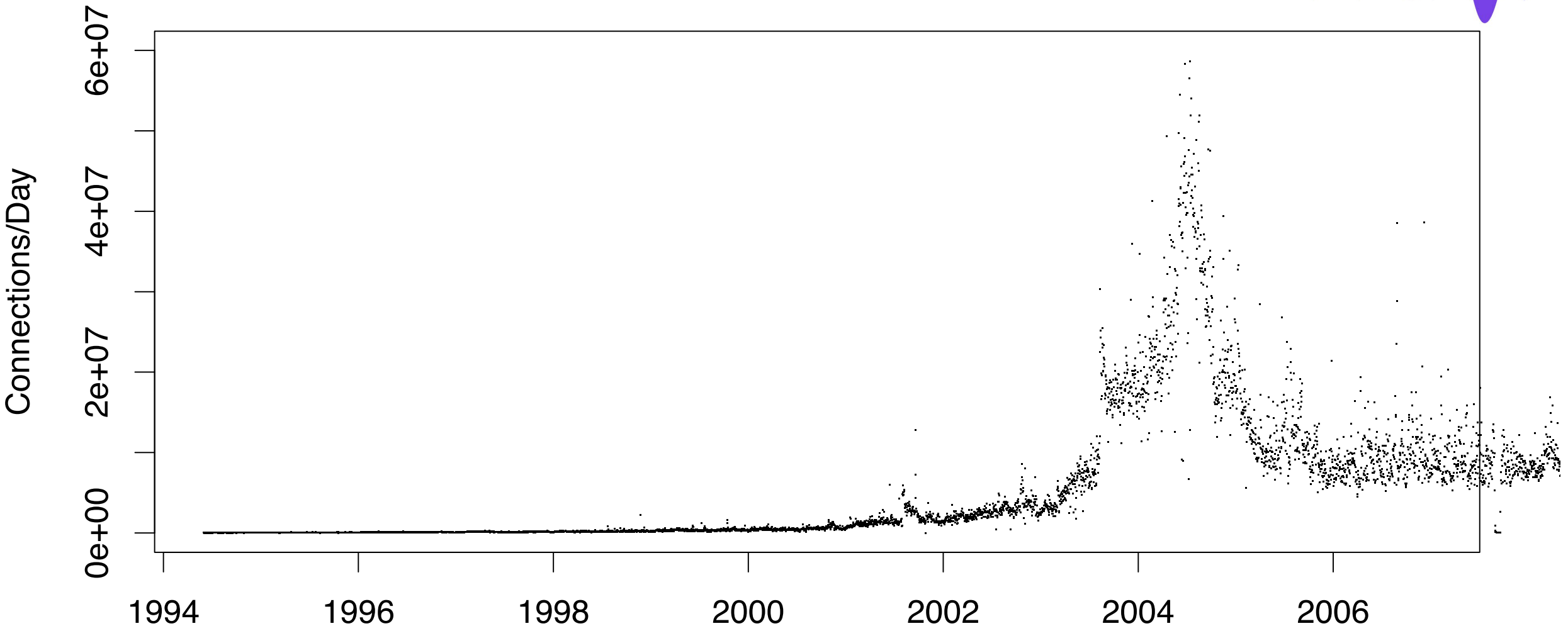
Data courtesy Aashish Sharma, Jay Krous, James Welcher & Partha Bannerjee

Evolution of Inbound Connections Per Day (LBNL)

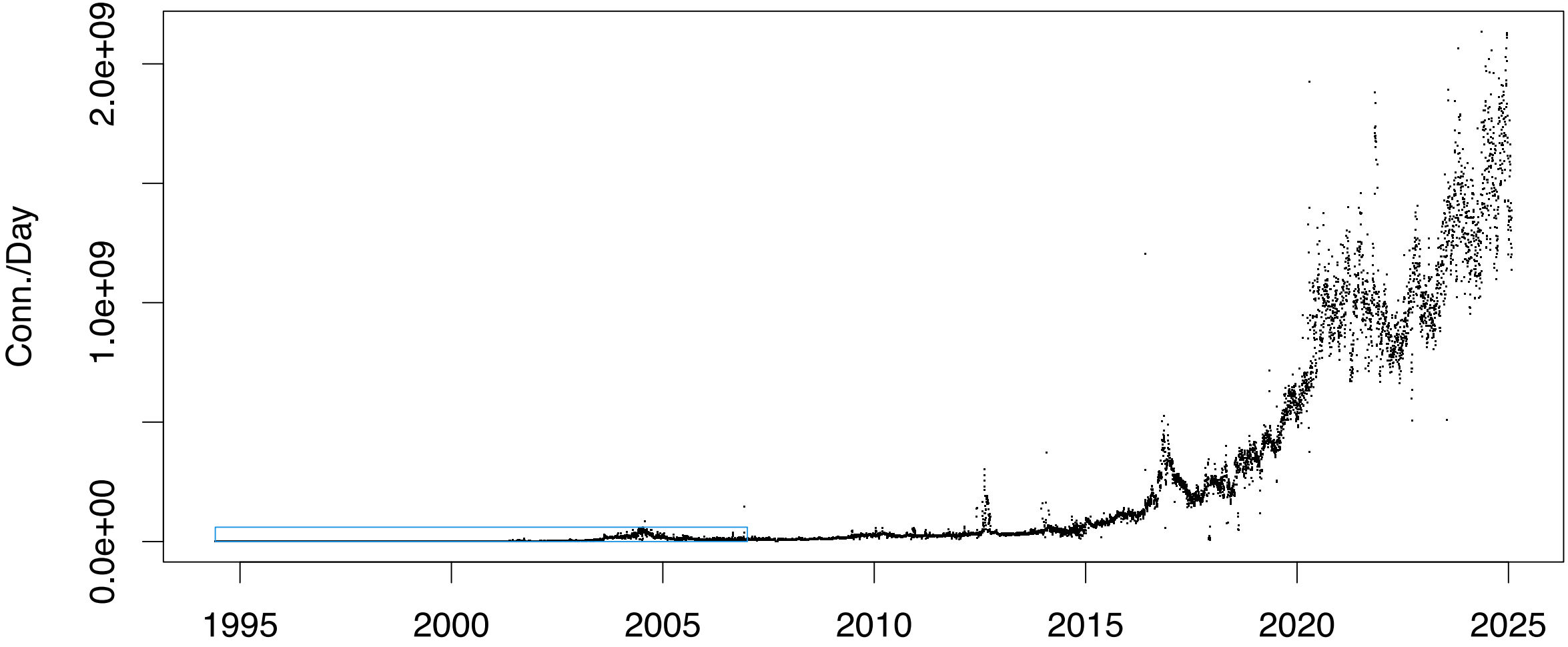


Data courtesy Aashish Sharma, Jay Krous, James Welcher & Partha Bannerjee

Evolution of Connections/Day (LBNL)

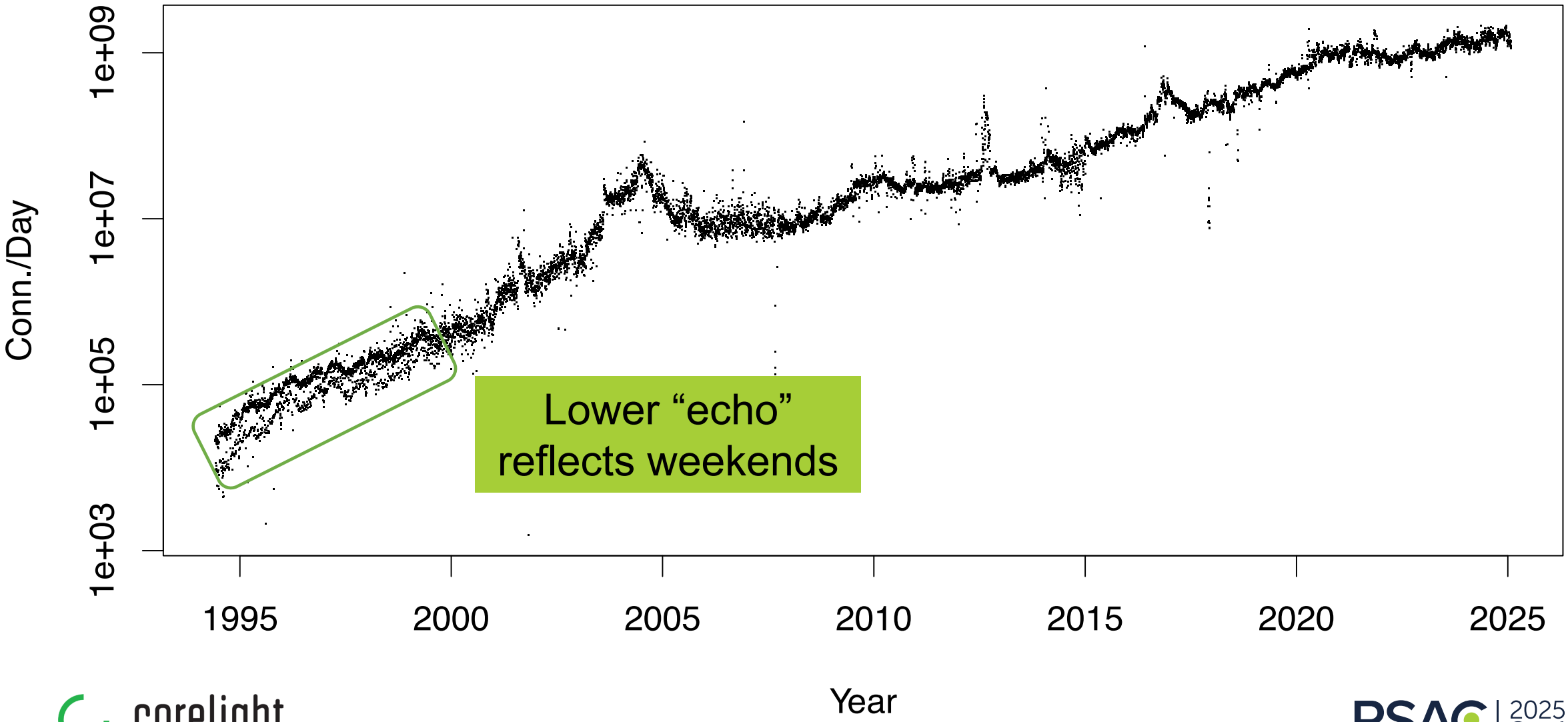


Evolution of Inbound Connections Per Day (LBNL)

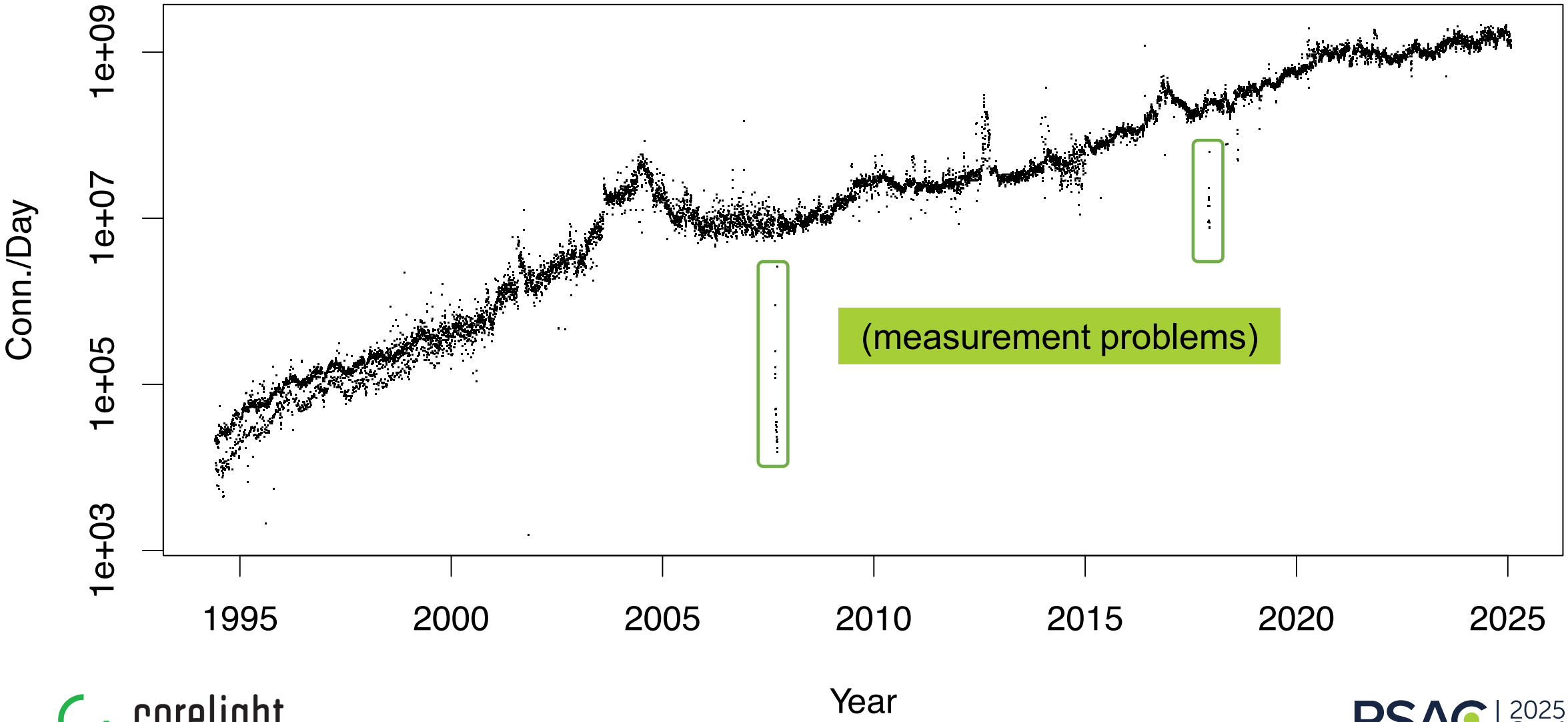


Data courtesy Aashish Sharma, Jay Krous, James Welcher & Partha Bannerjee

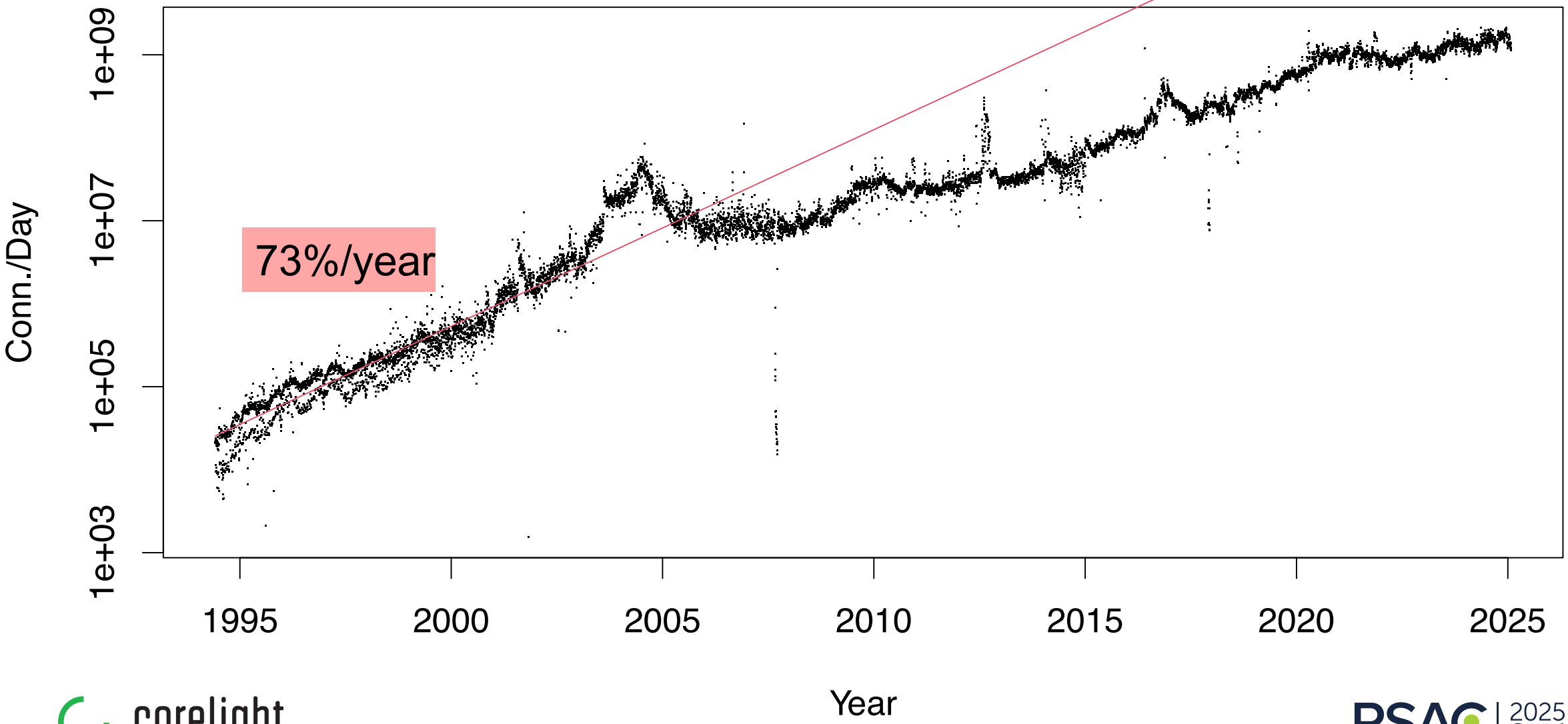
Evolution of Inbound Connections Per Day (LBNL)



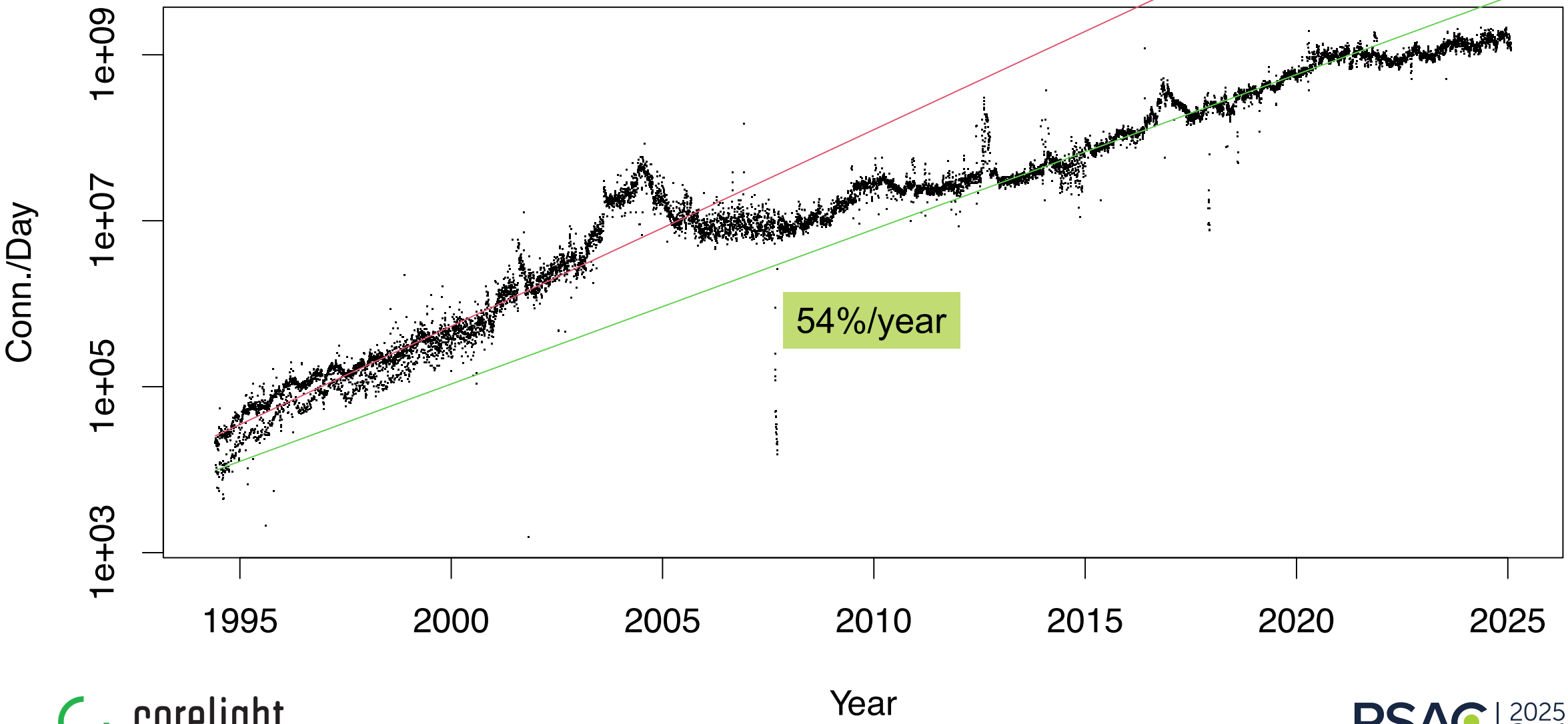
Evolution of Inbound Connections Per Day (LBNL)



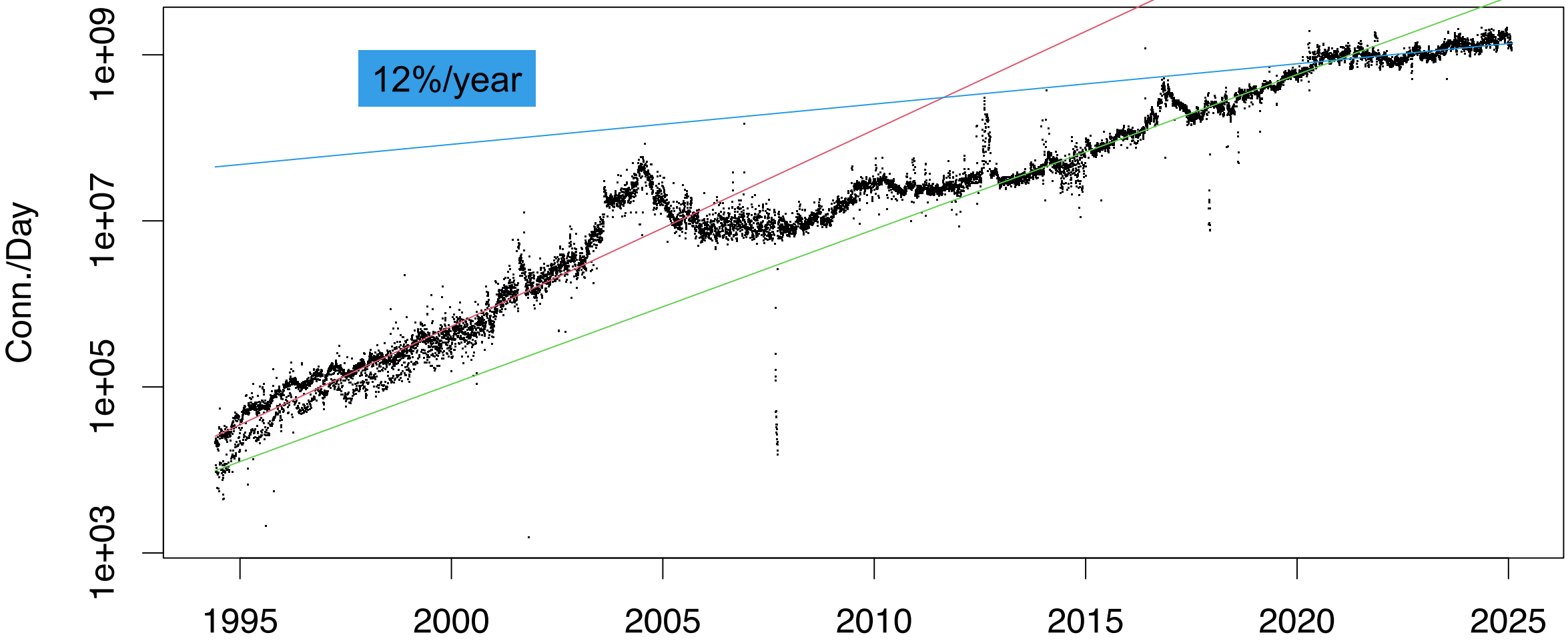
Evolution of Inbound Connections Per Day (LBNL)



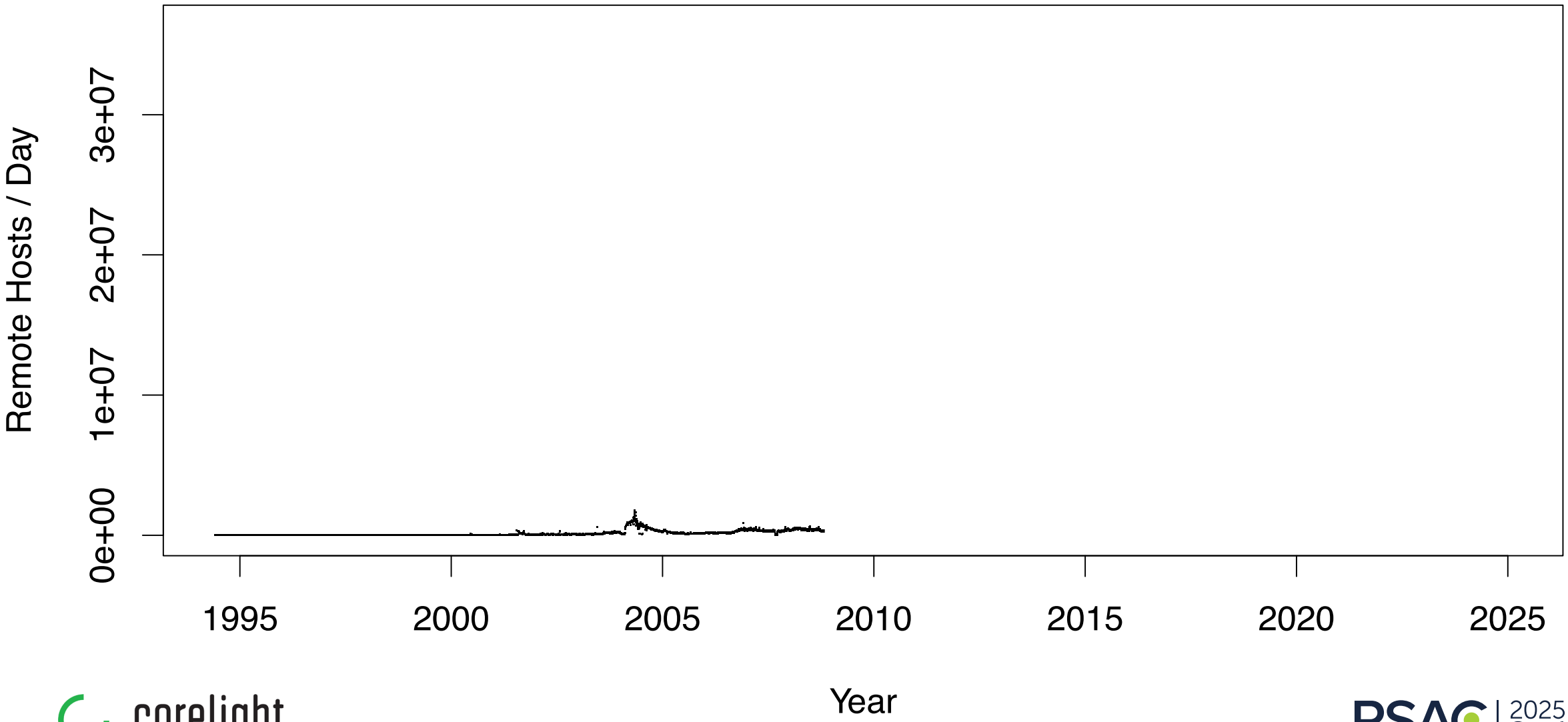
Evolution of Inbound Connections Per Day (LBNL)



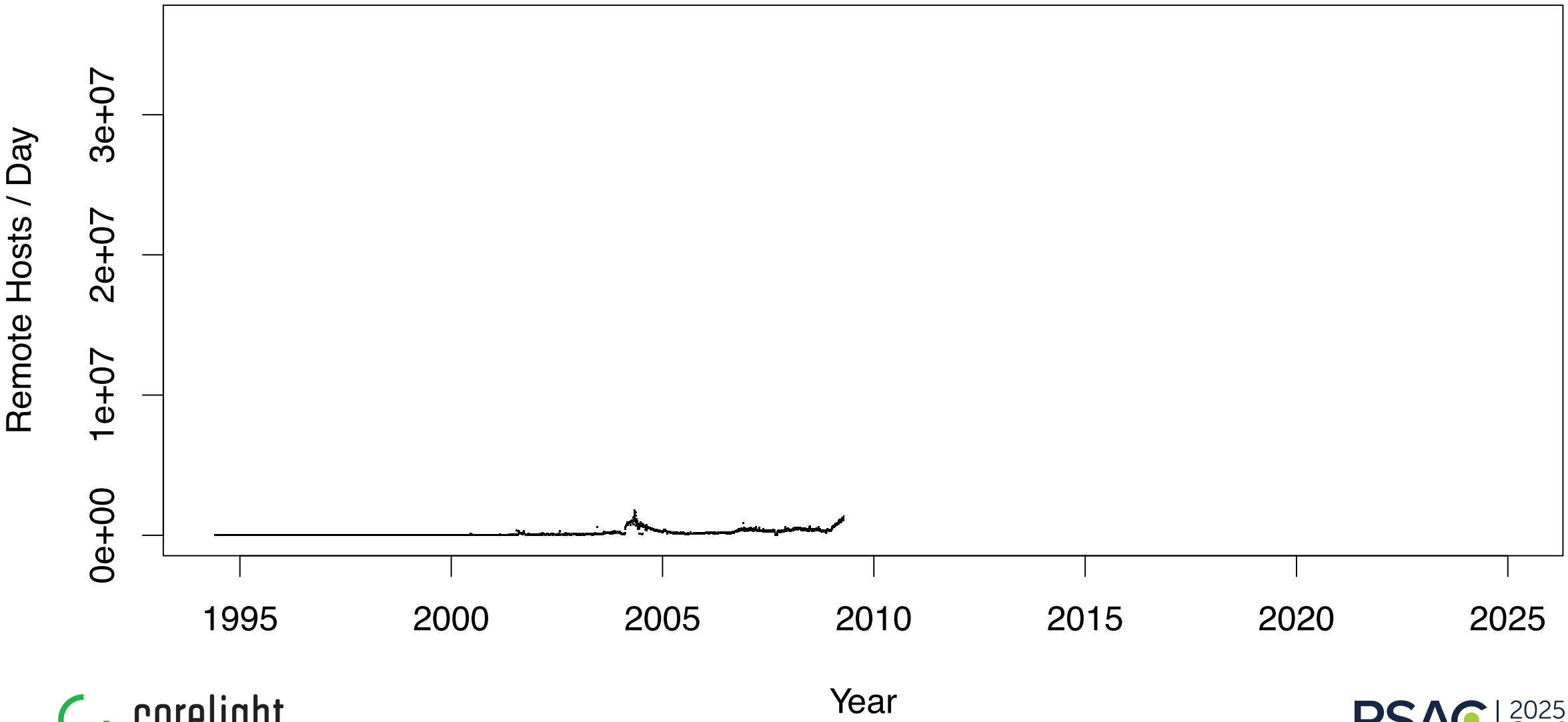
Evolution of Inbound Connections Per Day (LBNL)



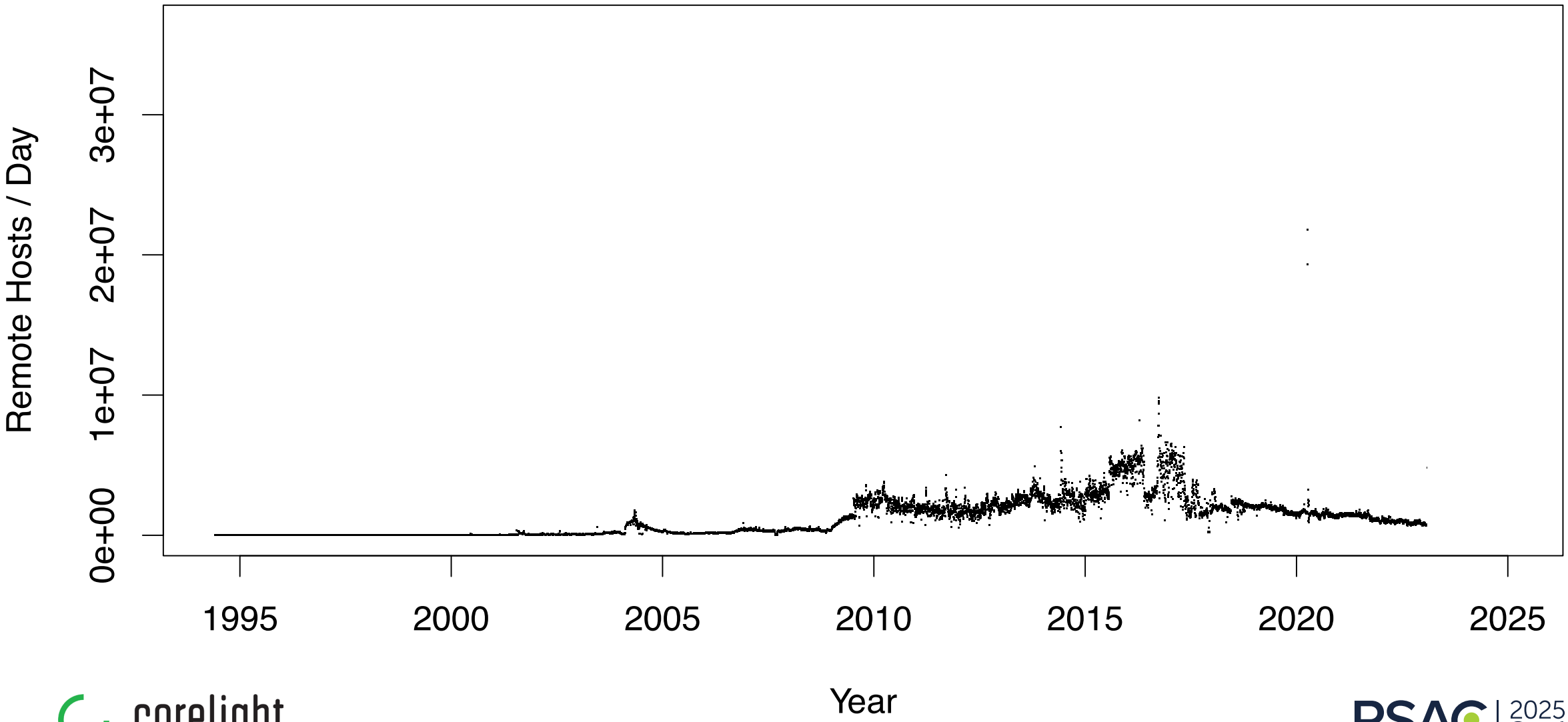
Evolution of Remote Hosts Per Day (LBNL)



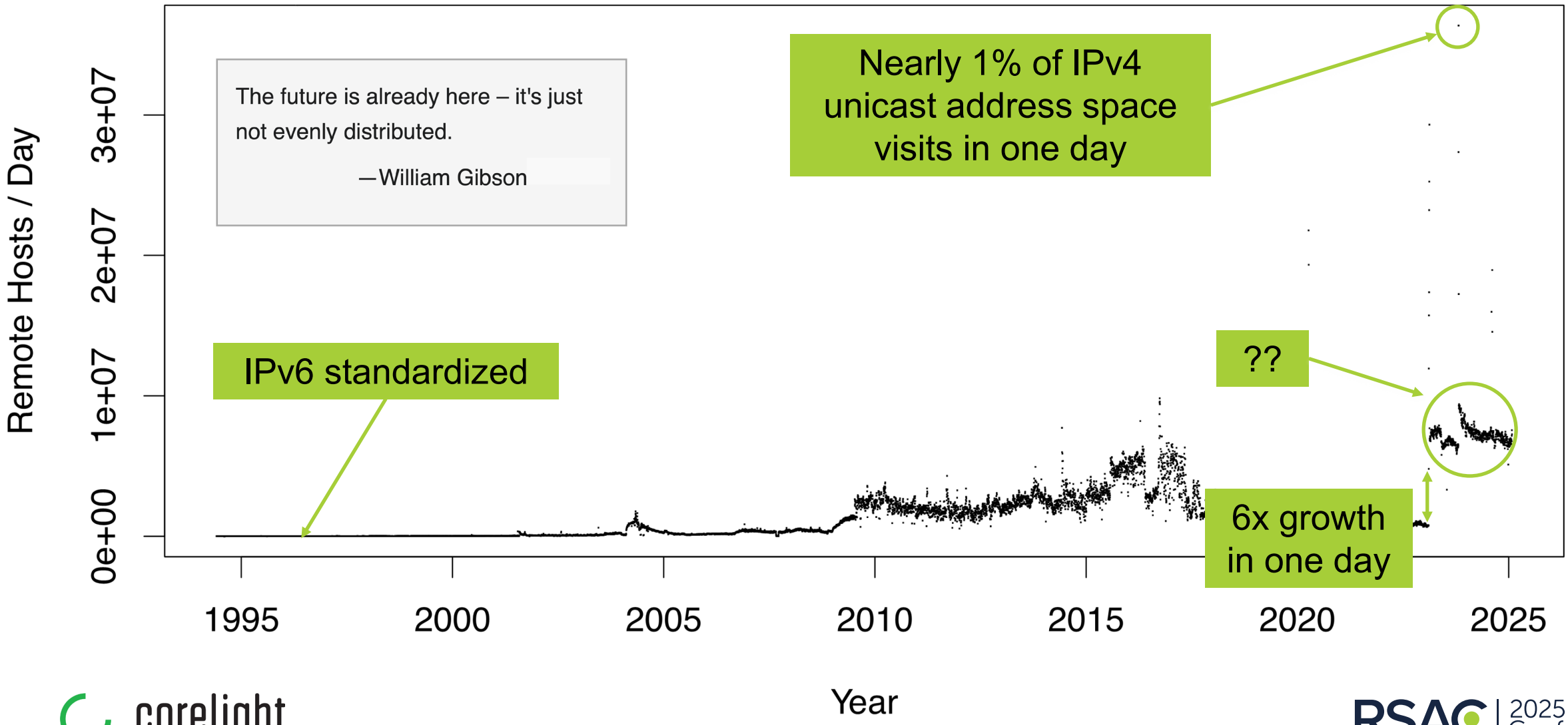
Evolution of Remote Hosts Per Day (LBNL)



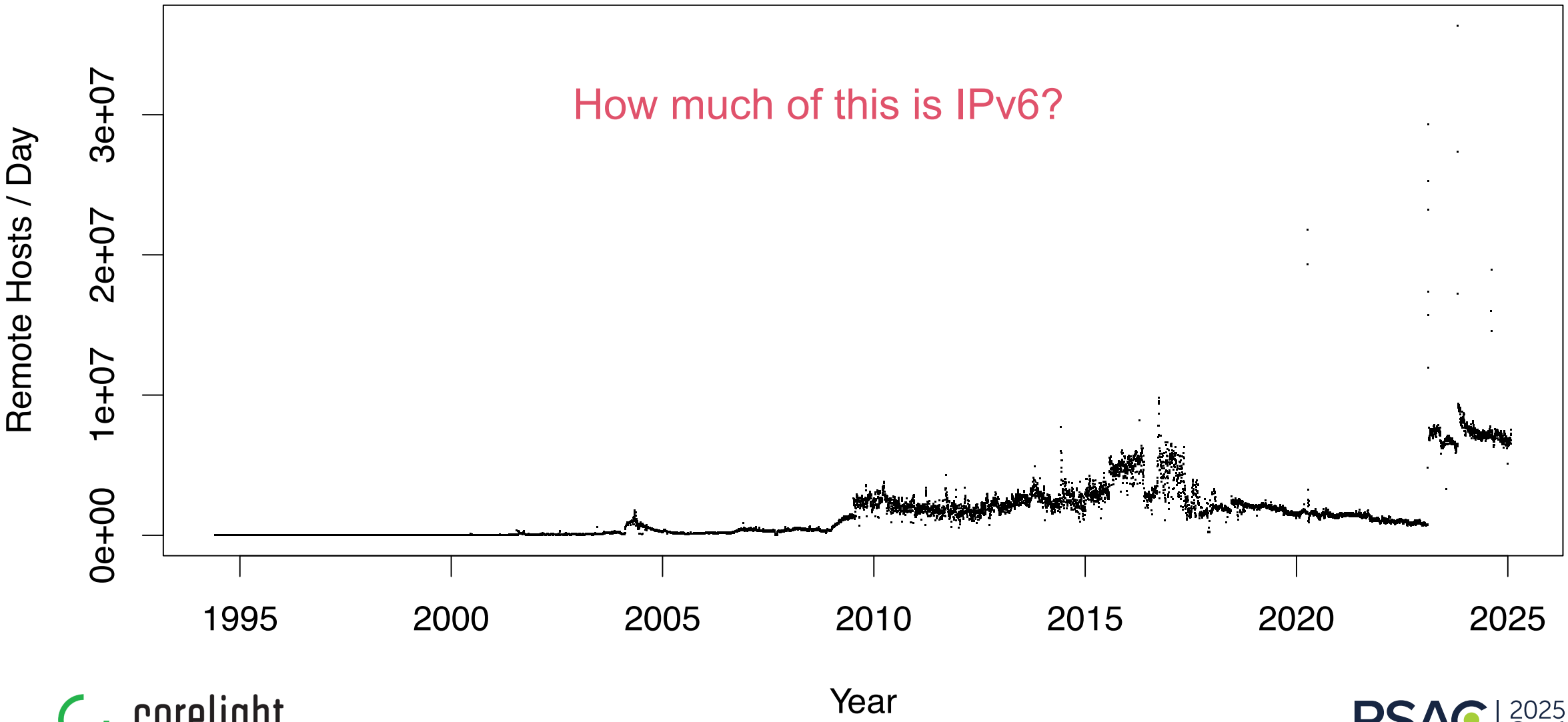
Evolution of Remote Hosts Per Day (LBNL)



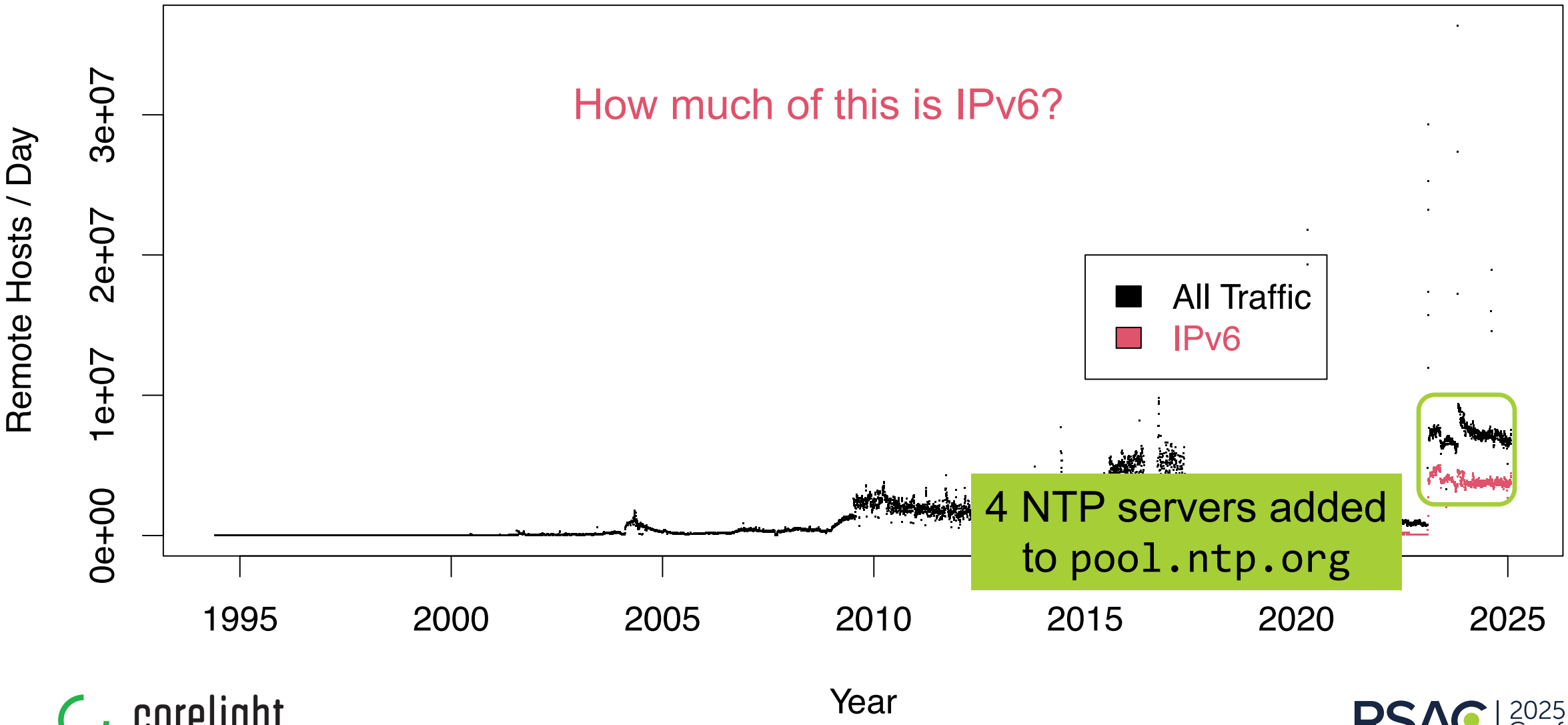
Evolution of Remote Hosts Per Day (LBNL)



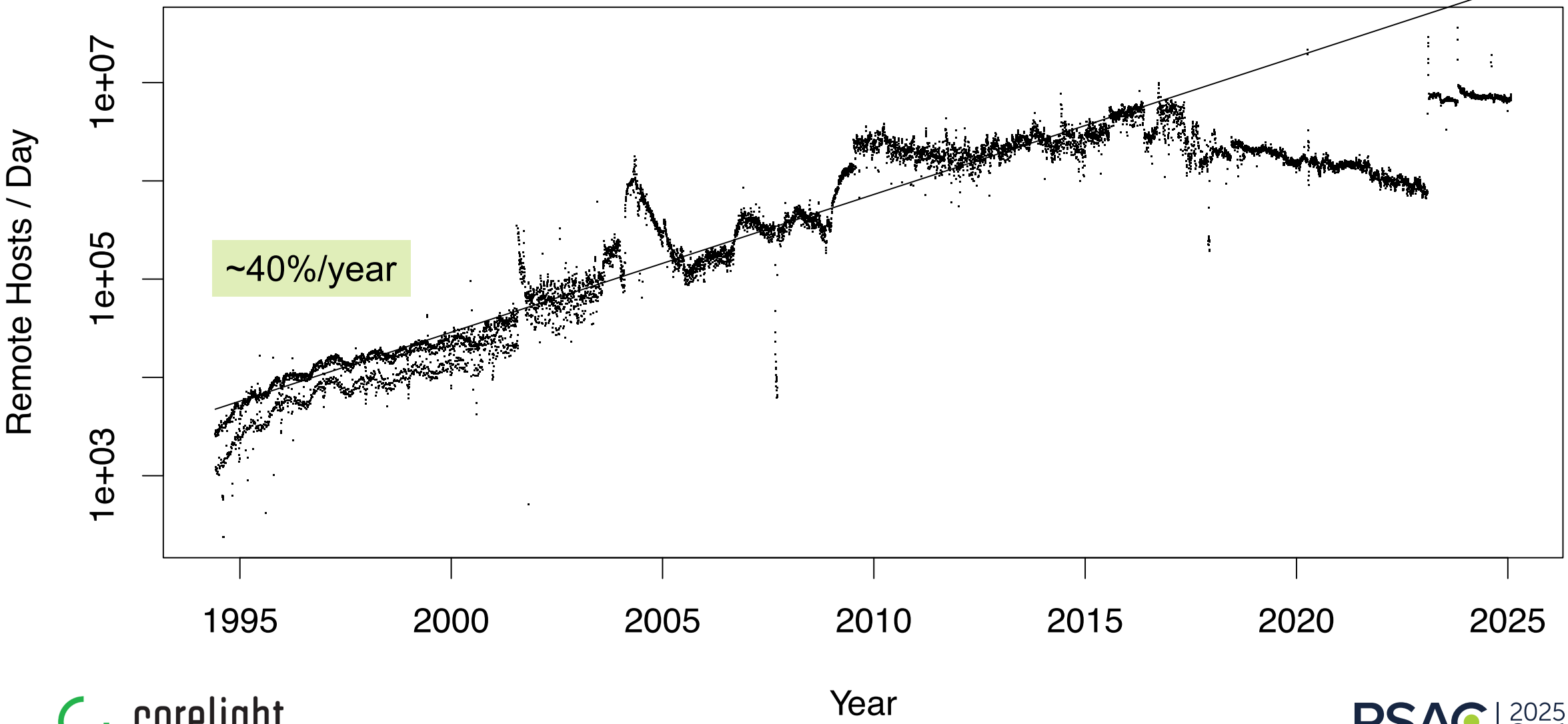
Evolution of Remote Hosts Per Day (LBNL)



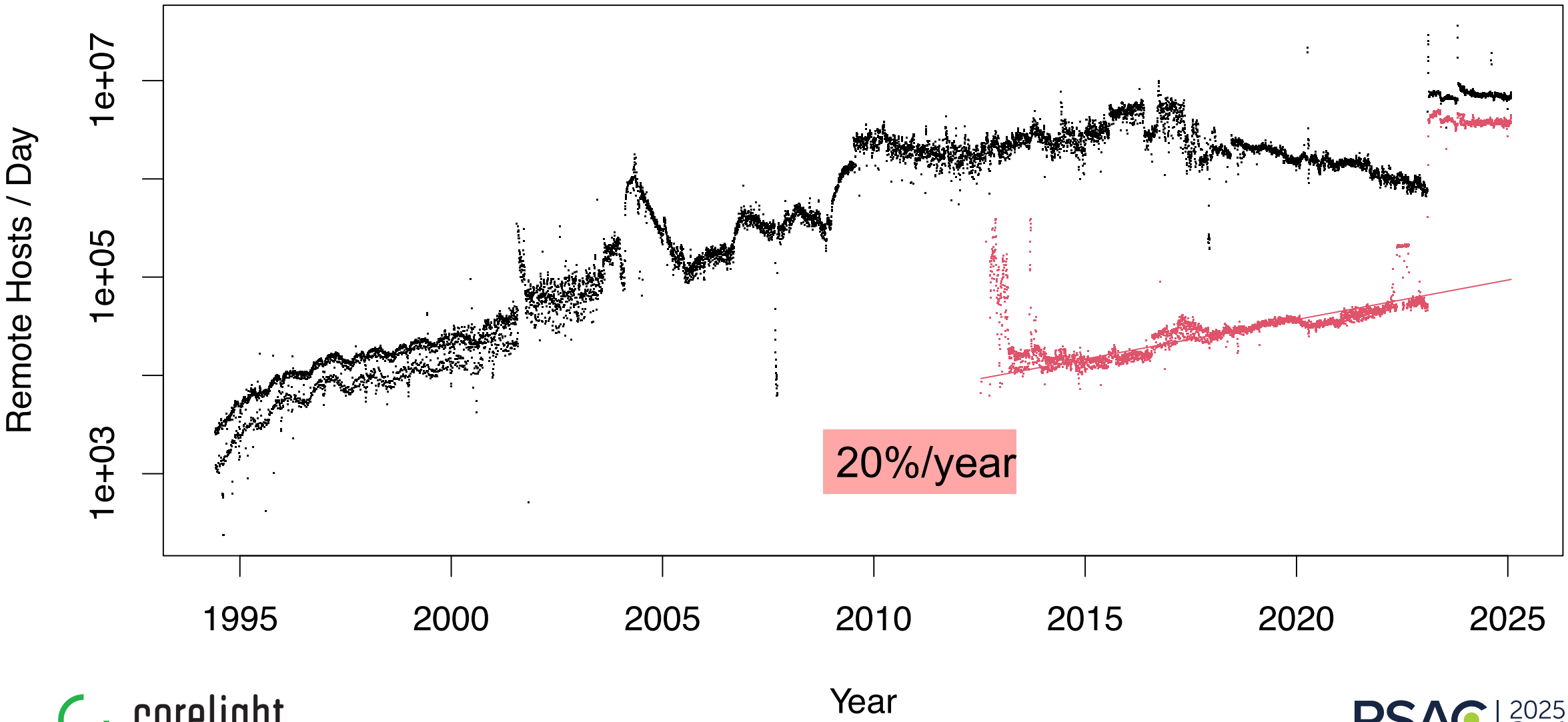
Evolution of Remote Hosts Per Day (LBNL)



Evolution of Remote Hosts Per Day (LBNL)



Evolution of Remote Hosts Per Day (LBNL)



Proportion of *productive connections* as of late 2023

Site	IPv6 %
LBNL	?

Proportion of *productive connections* as of late 2023

Site	IPv6 %
LBNL	62

!

Proportion of *productive connections* as of late 2023

Site	IPv6 %
LBNL	62.2

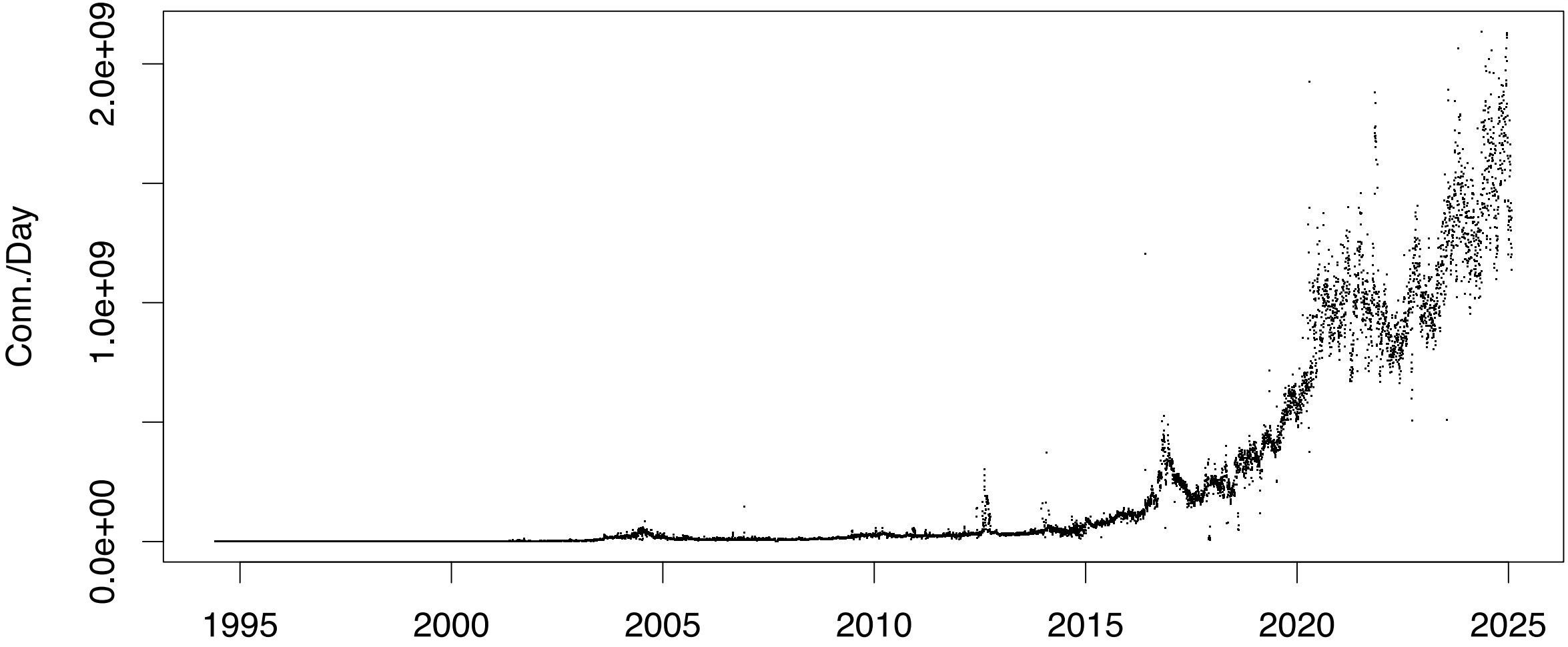
w/o NTP (network time)
& DNS (name lookups)

Proportion of *productive connections* as of late 2023

Site	IPv6 %
LBNL	62/210

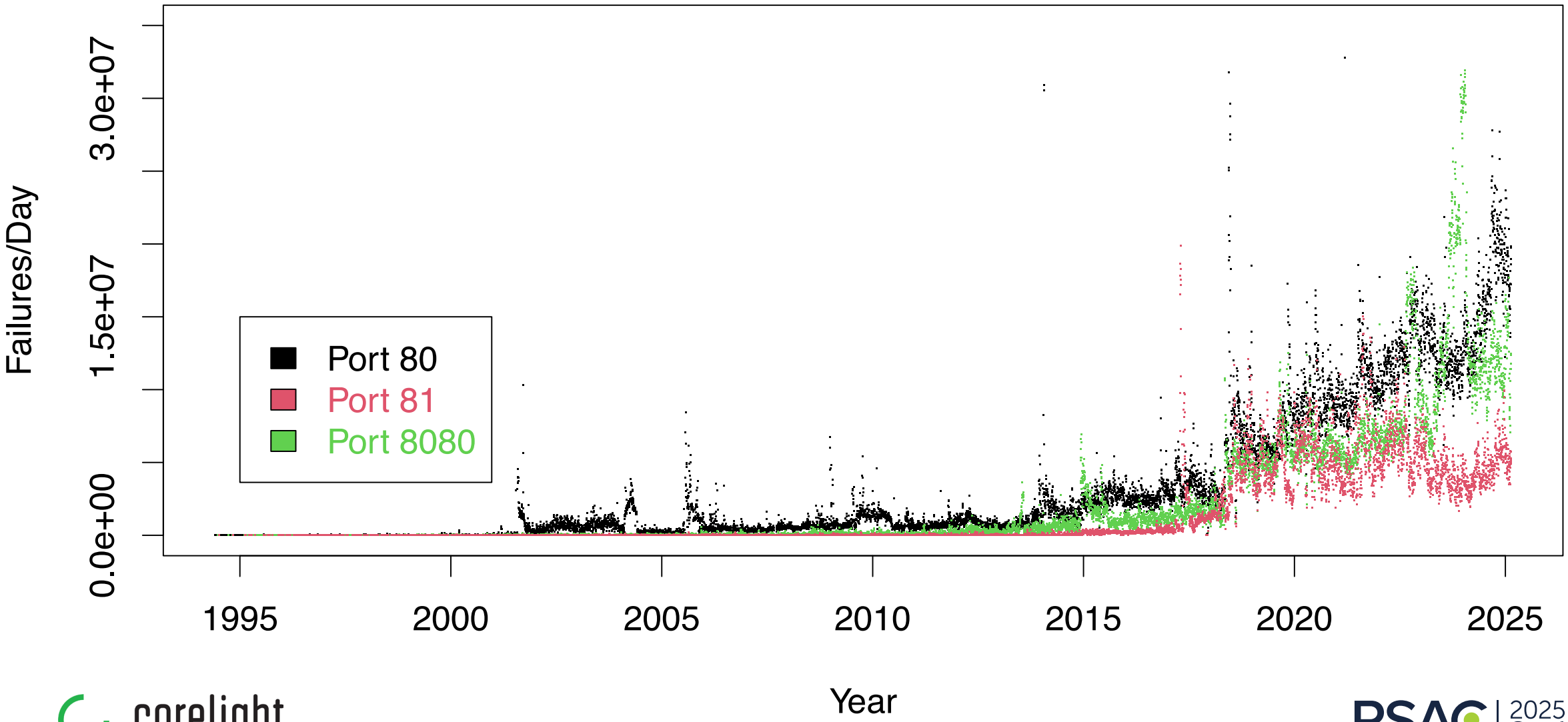
w/o NTP,
DNS & QUIC

Evolution of Inbound Connections Per Day (LBNL)

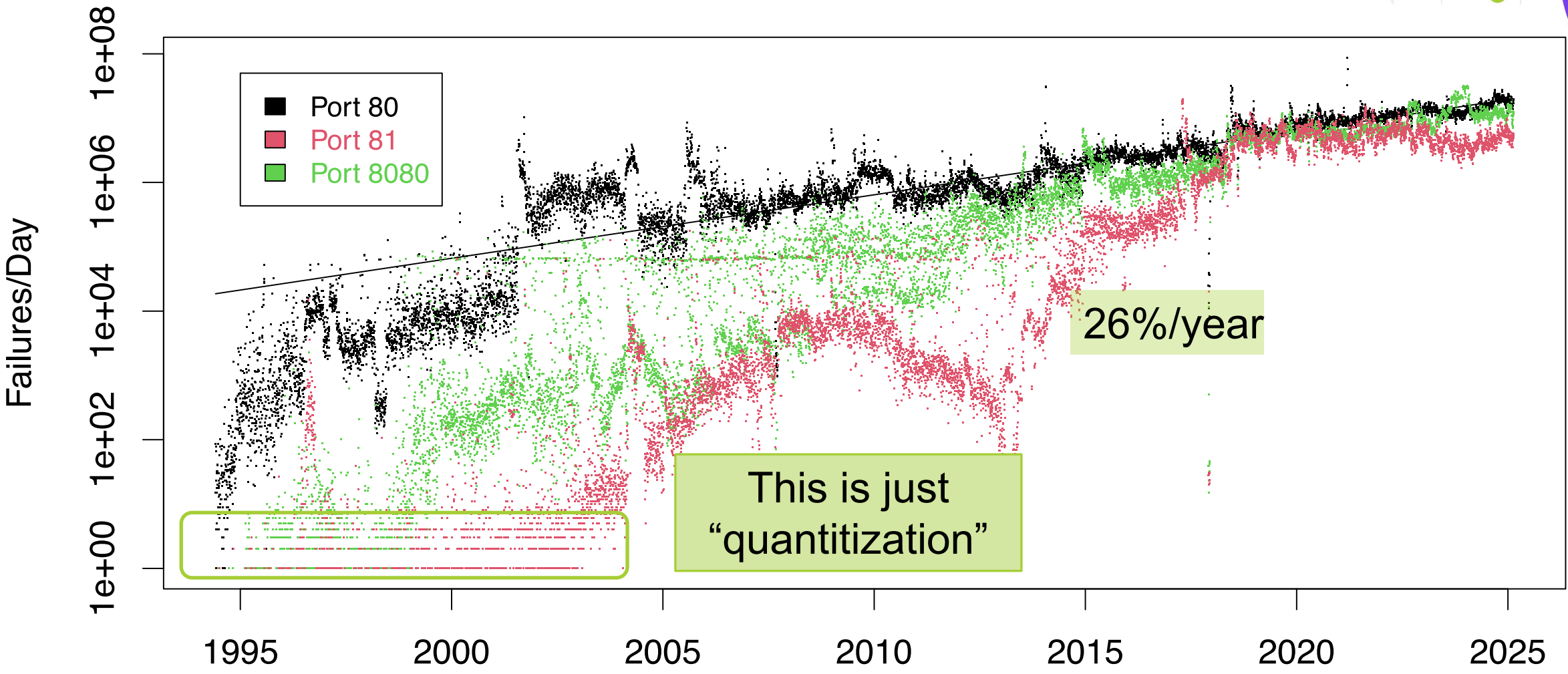


Data courtesy Aashish Sharma, Jay Krous, James Welcher & Partha Bannerjee

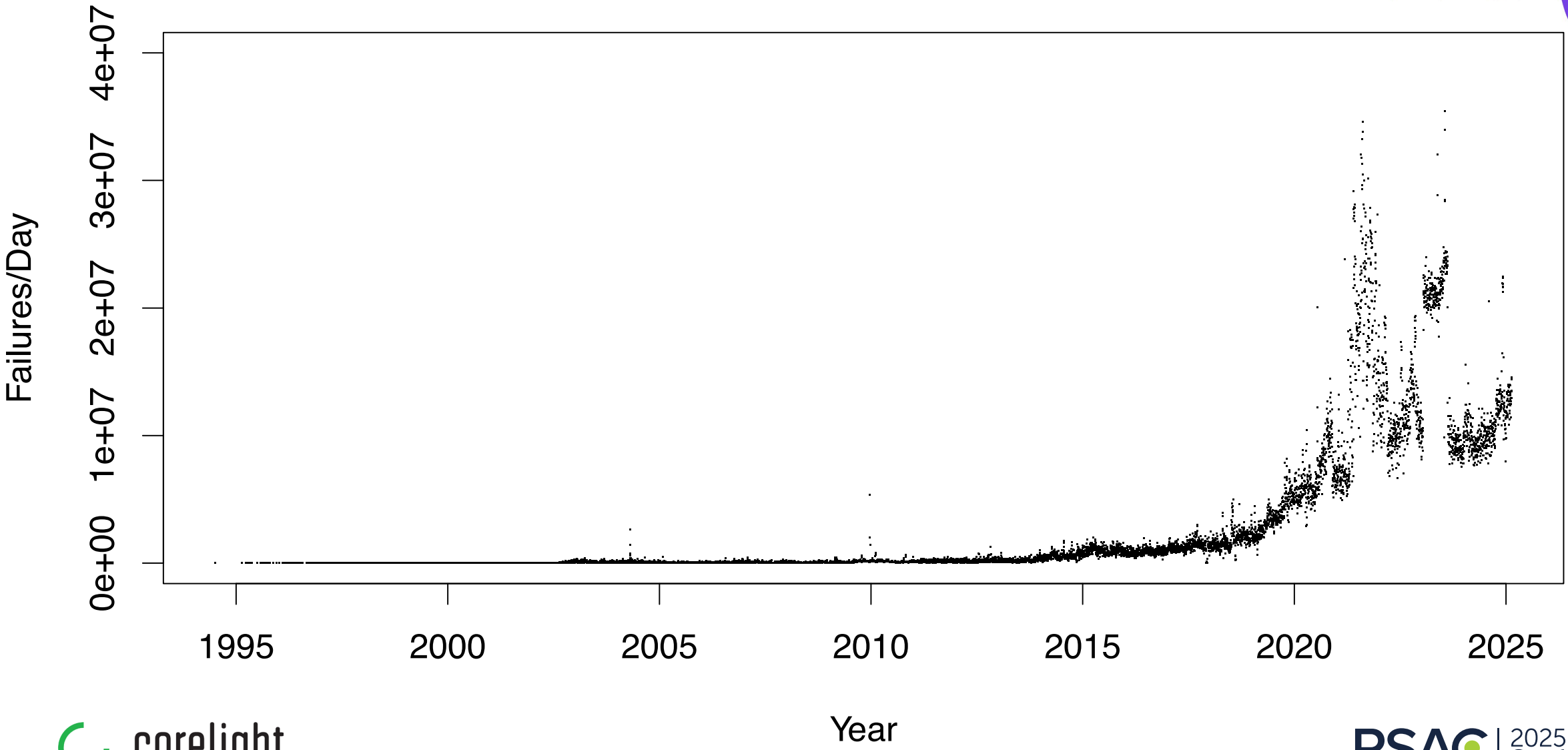
Web: HTTP Scans (80/81/8080)



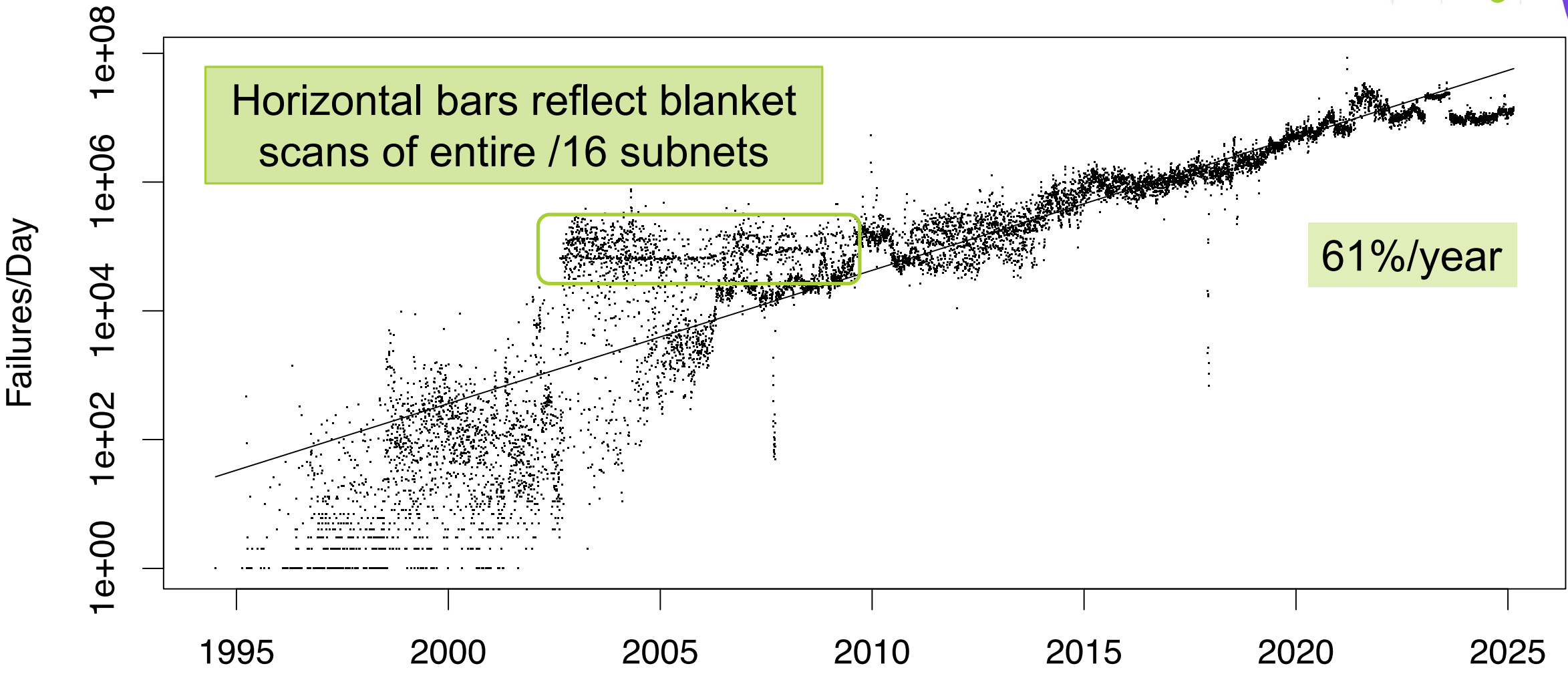
Web: HTTP Scans (80/81/8080)



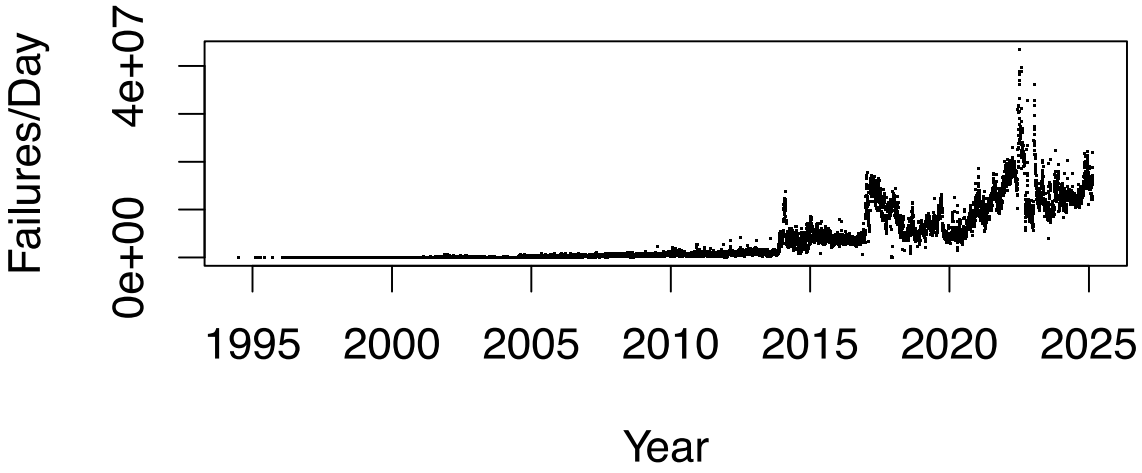
Encrypted Web: HTTPS



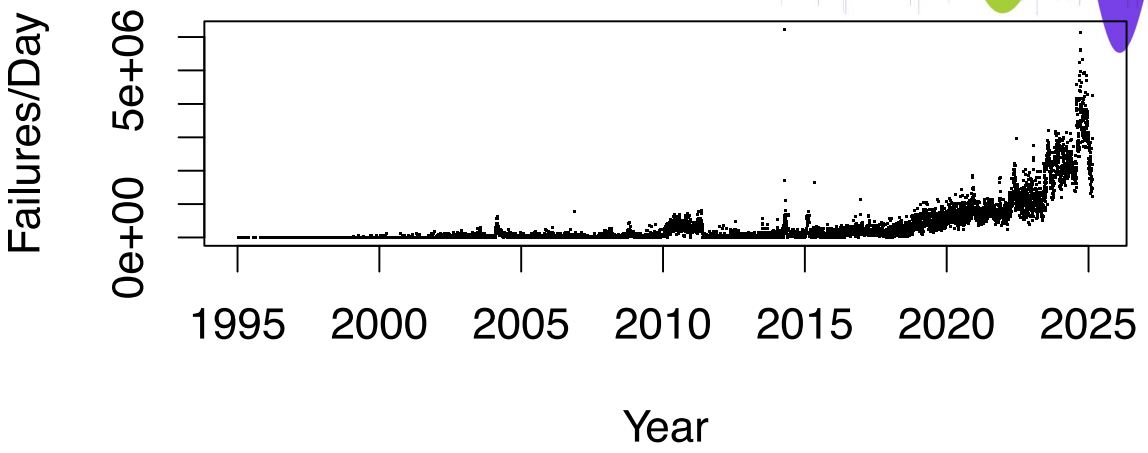
Encrypted Web: HTTPS



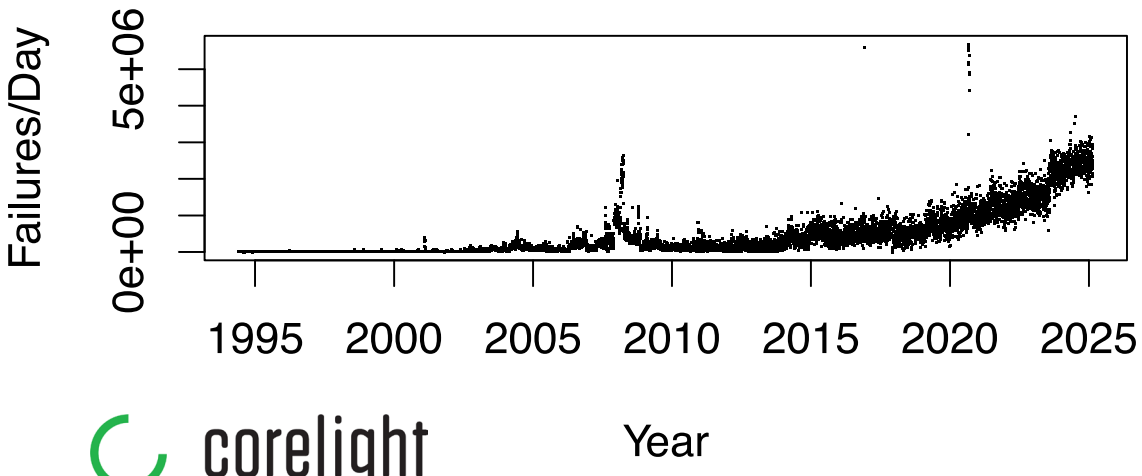
Secure Shell: SSH



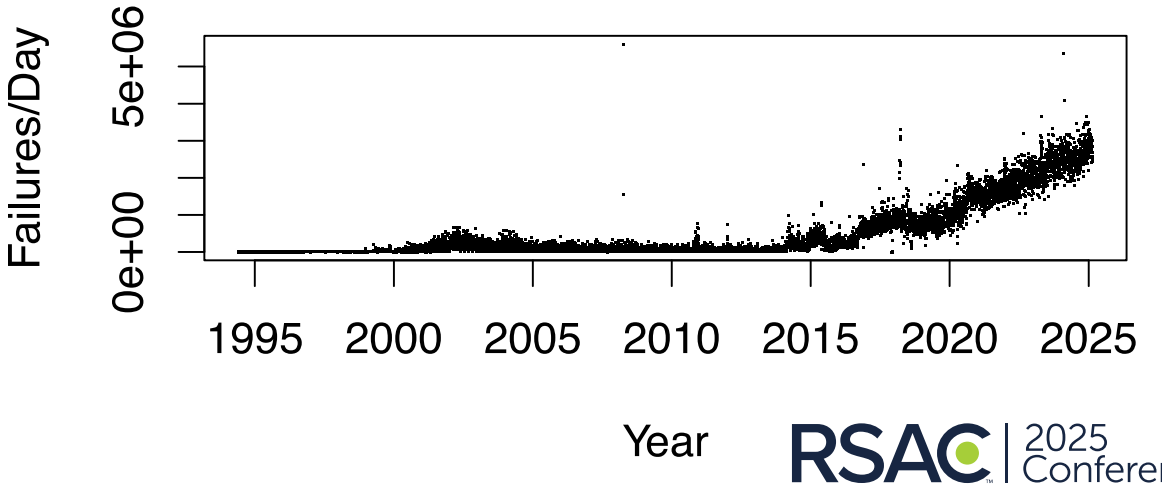
Proxy: SOCKS



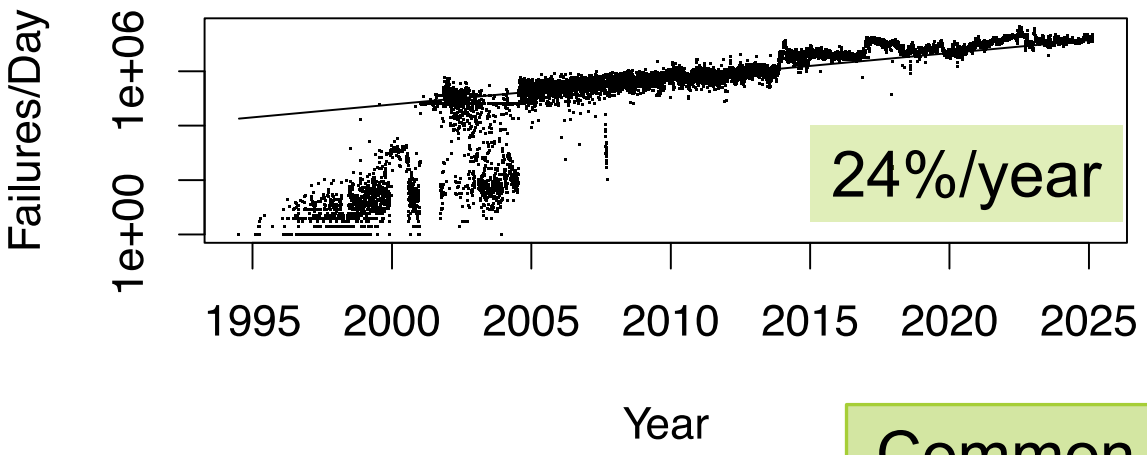
Email: SMTP



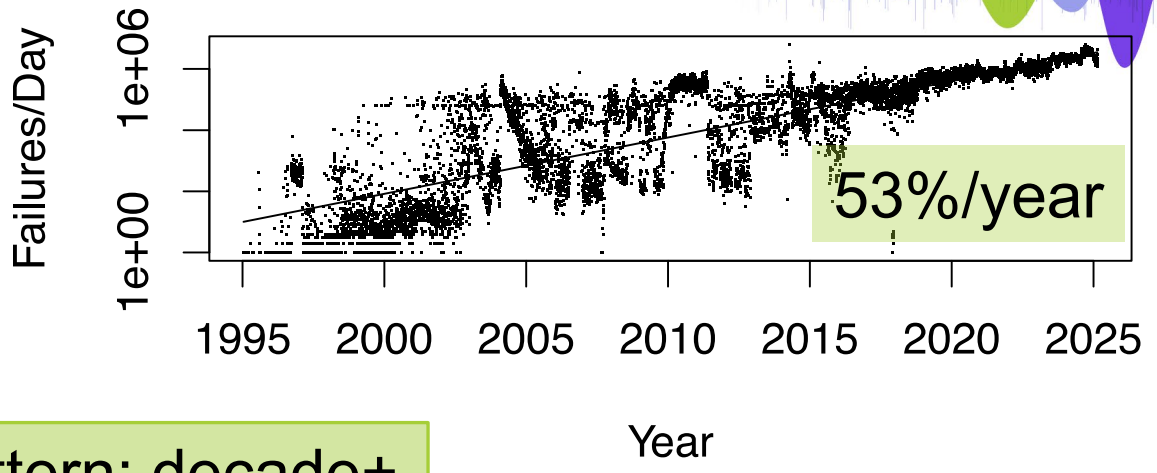
File Transfer: FTP



Secure Shell: SSH

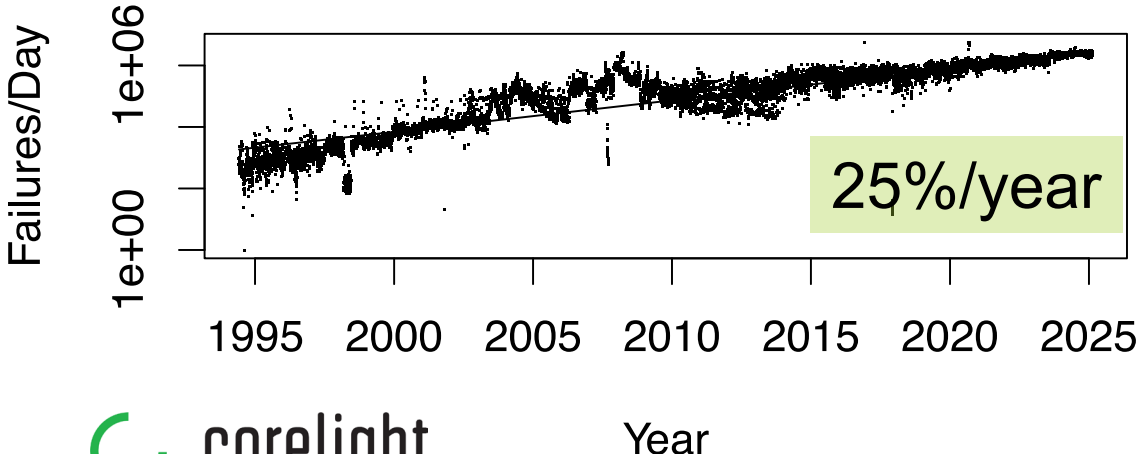


Proxy: SOCKS

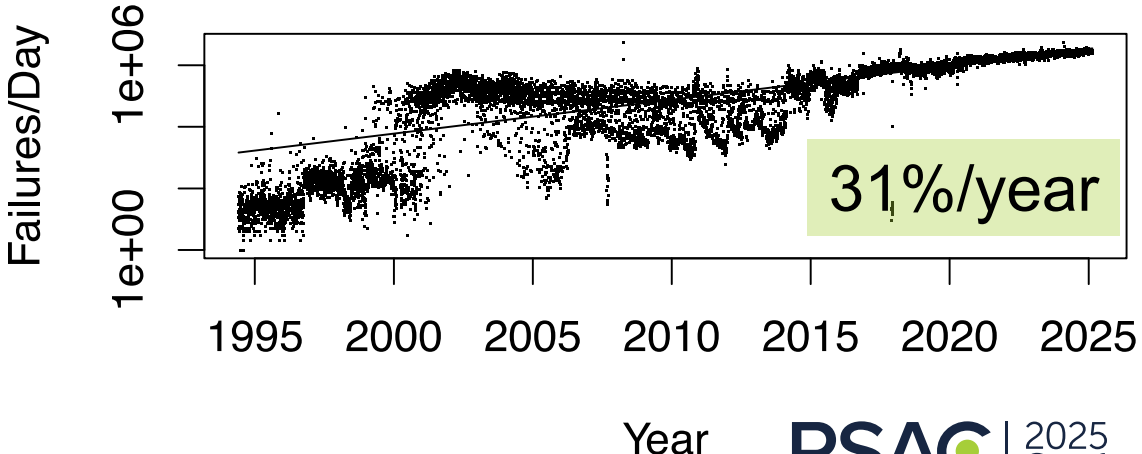


Common pattern: decade+ of sustained exponential growth in scanning

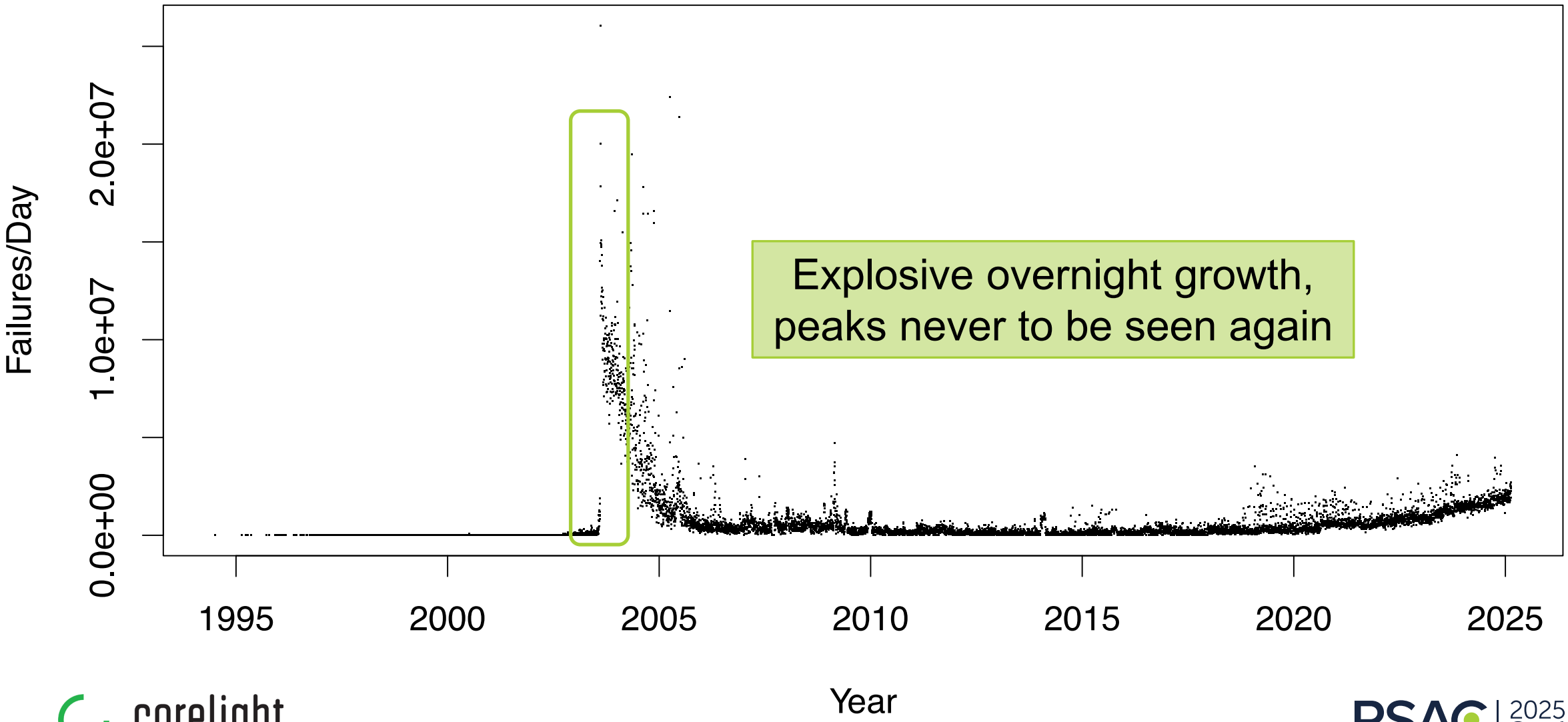
Email: SMTP



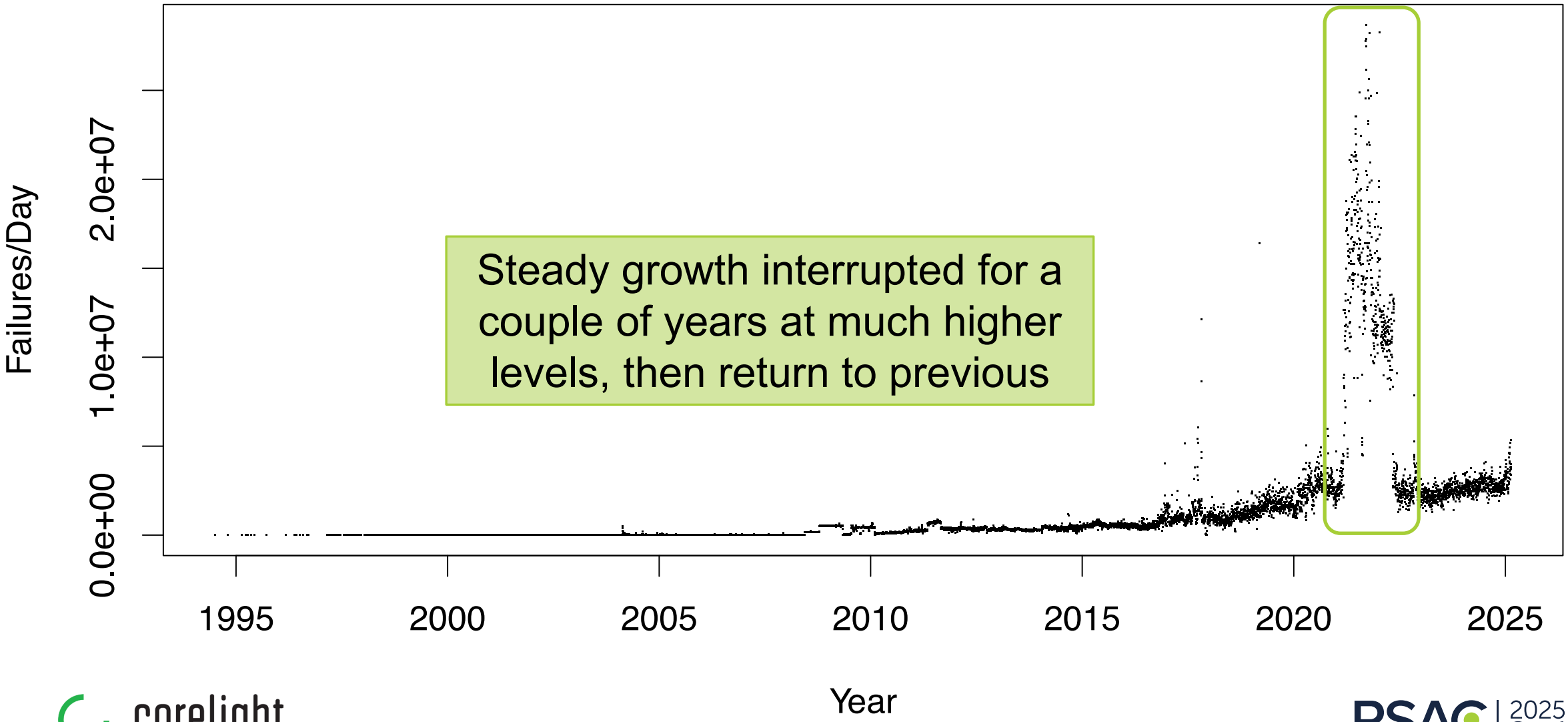
File Transfer: FTP



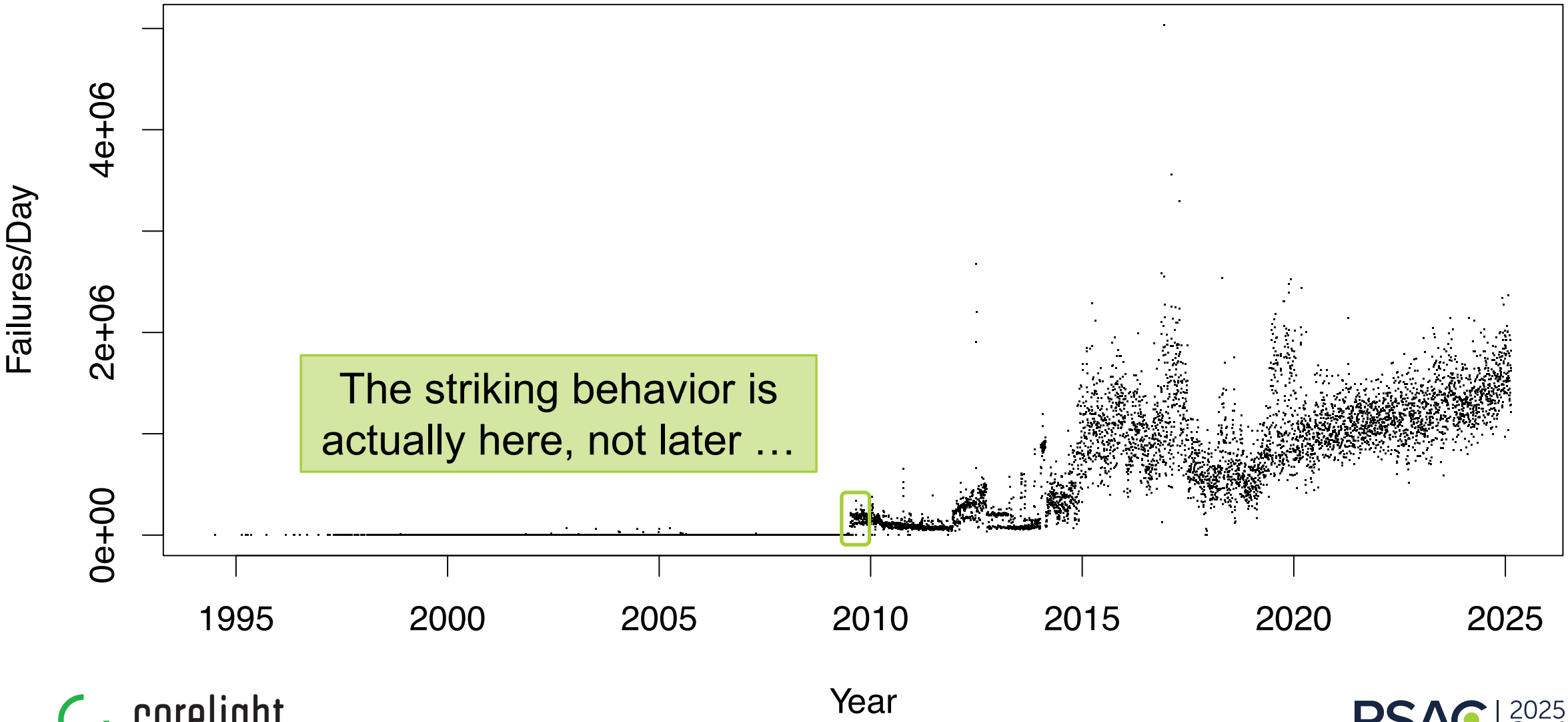
Windows Services: DCE/RPC



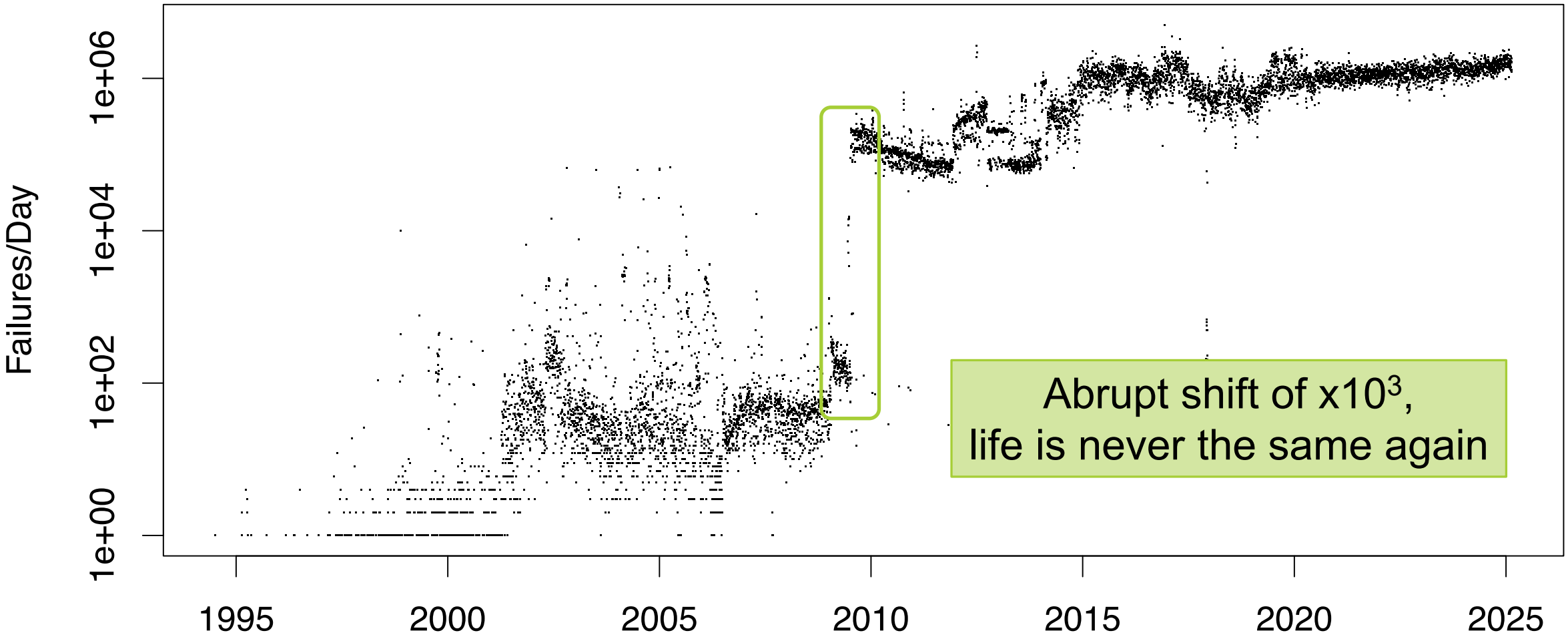
Active Directory: LDAP



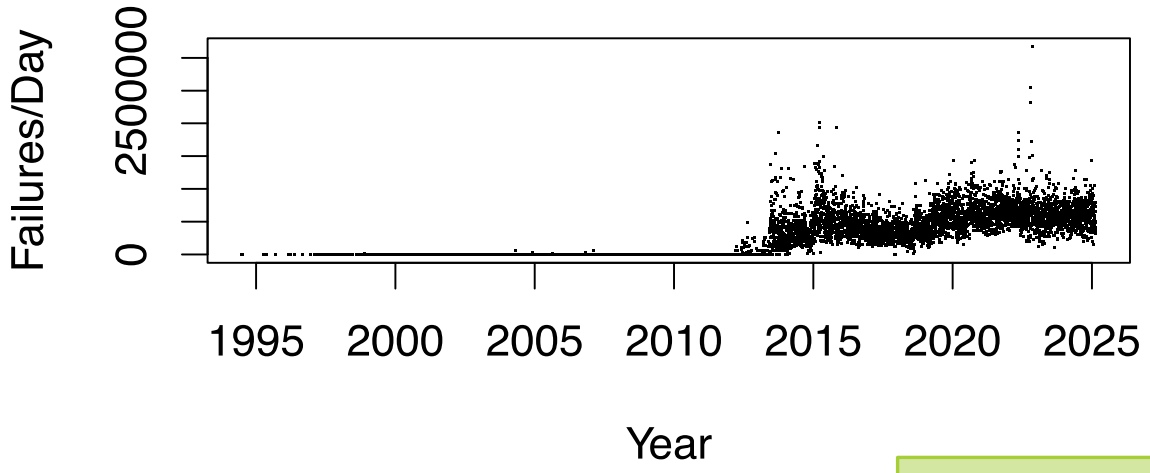
Windows NetBIOS (137)



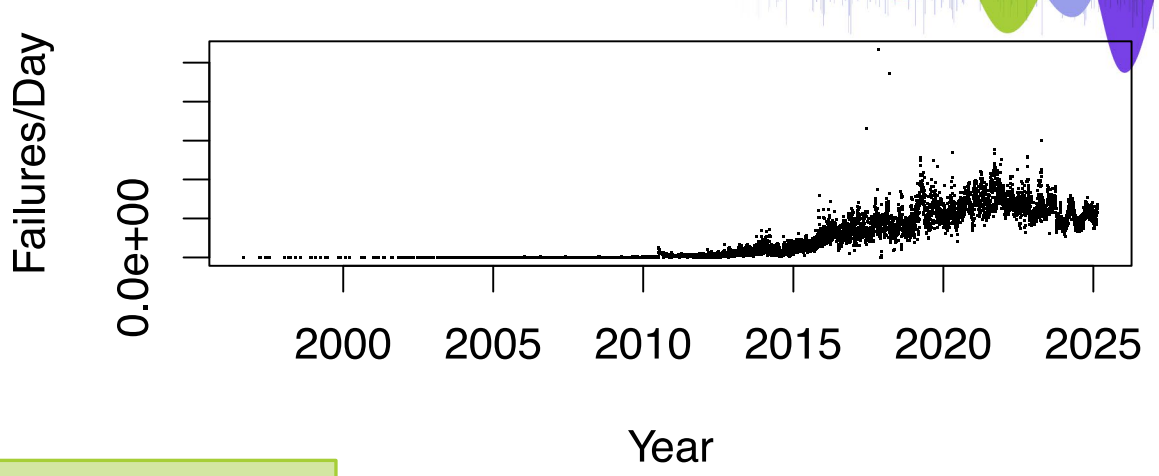
Windows NetBIOS (137)



Internet testing: Chargen

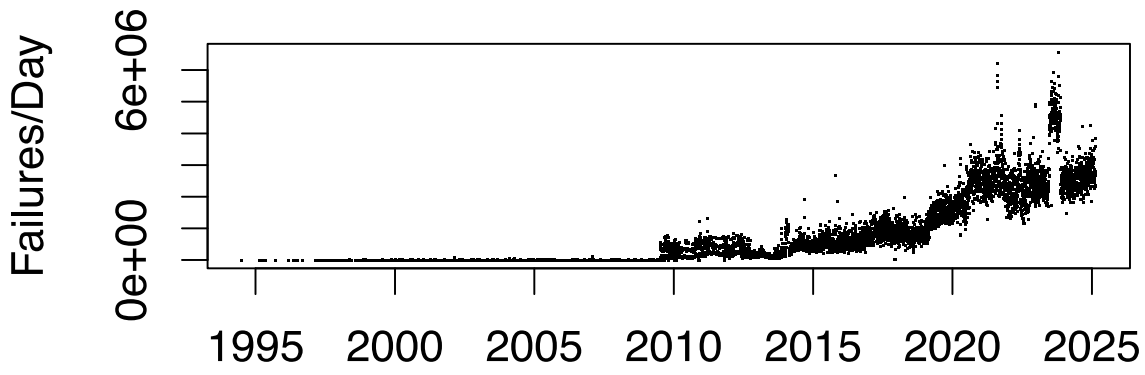


Telephony: SIP

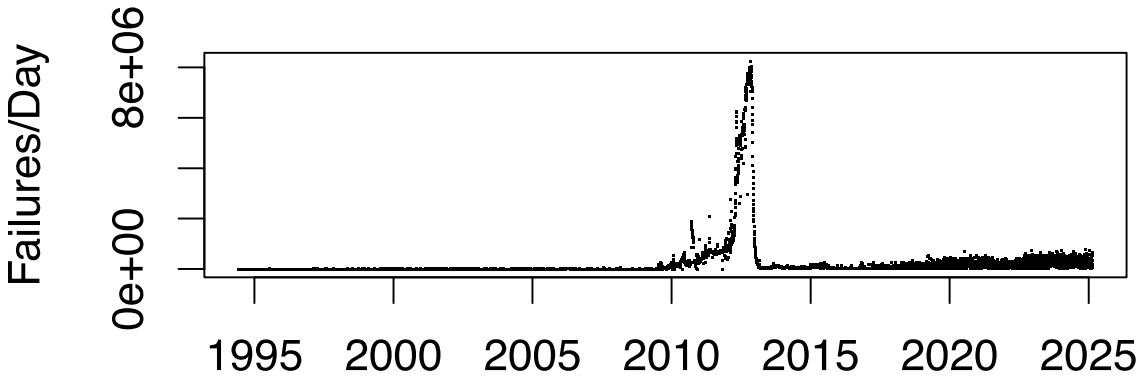


Same for all of these!

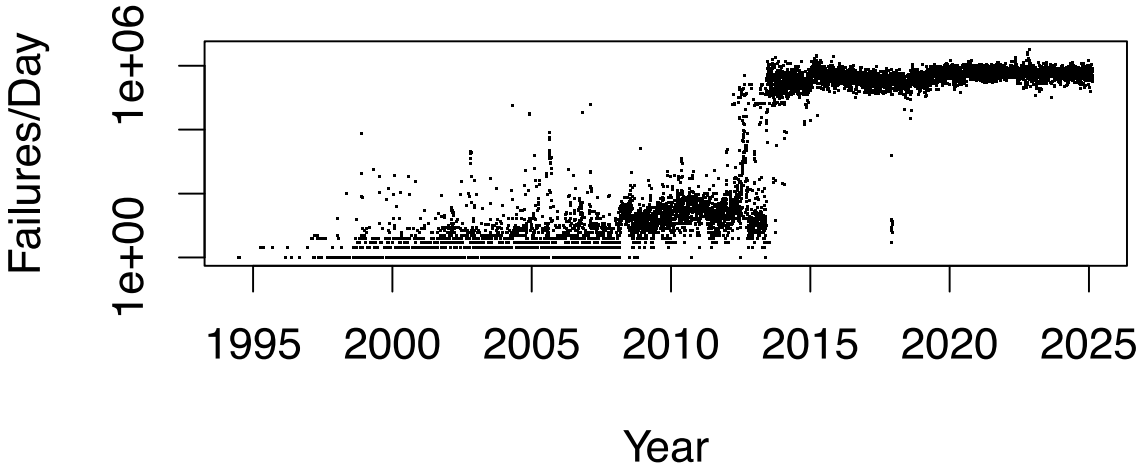
Network Management: SNMP



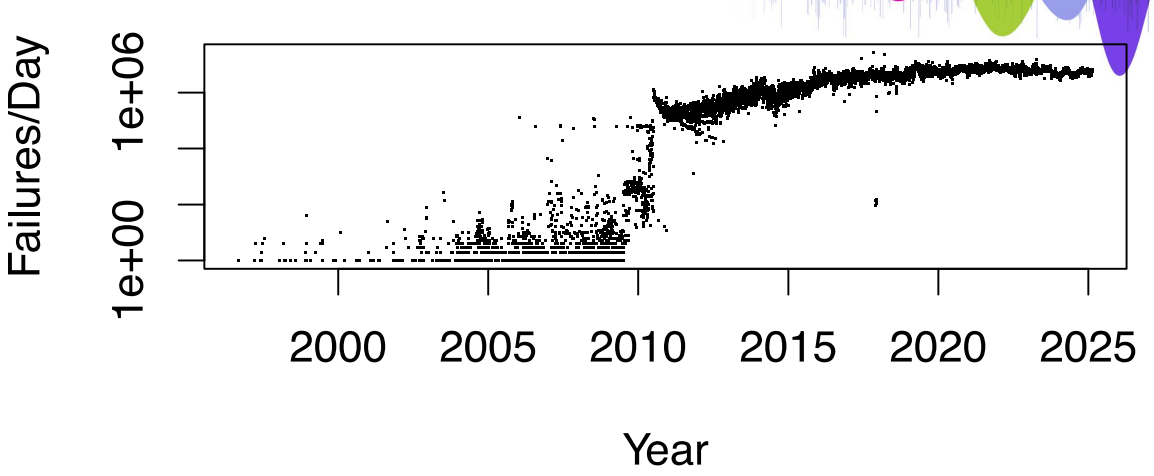
Unencrypted Remote Login: Shell



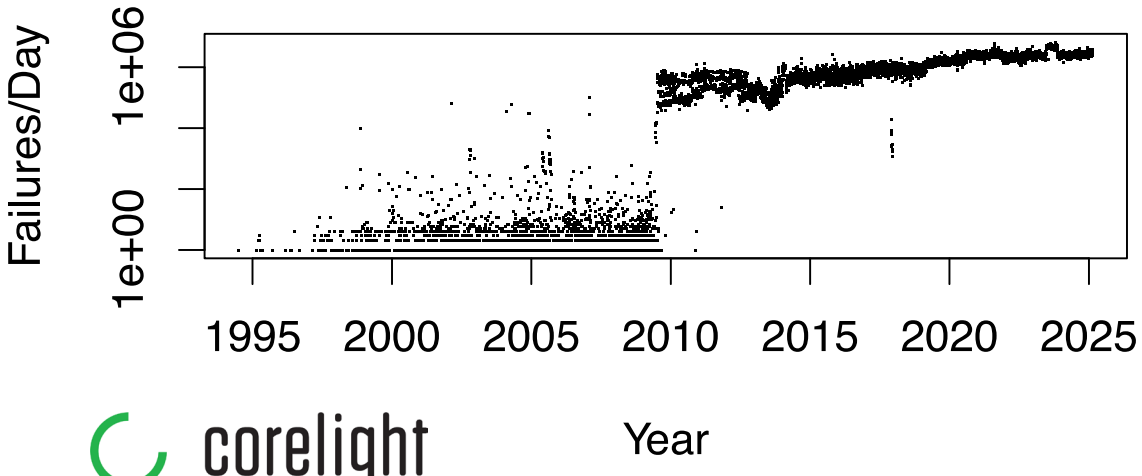
Internet testing: Chargen



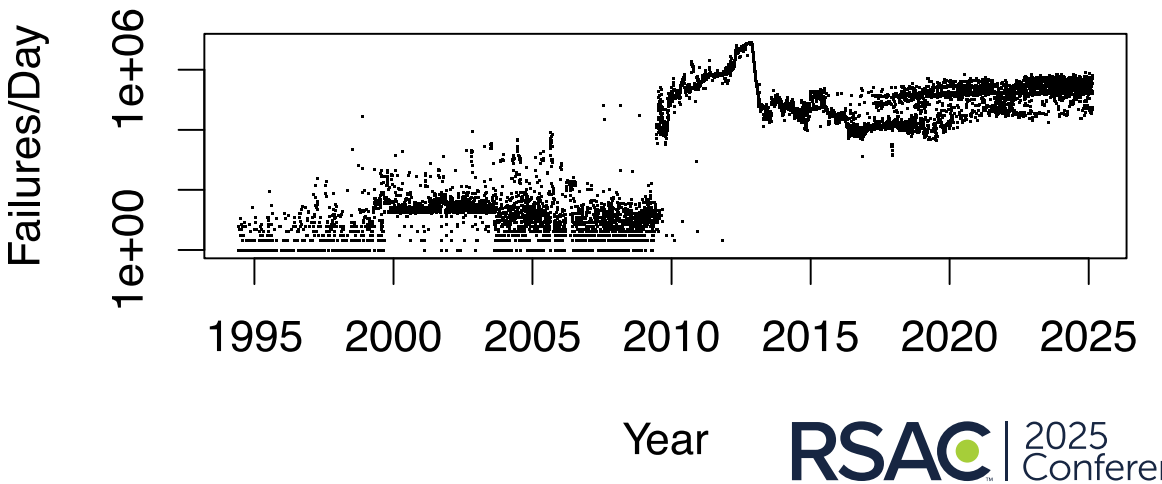
Telephony: SIP



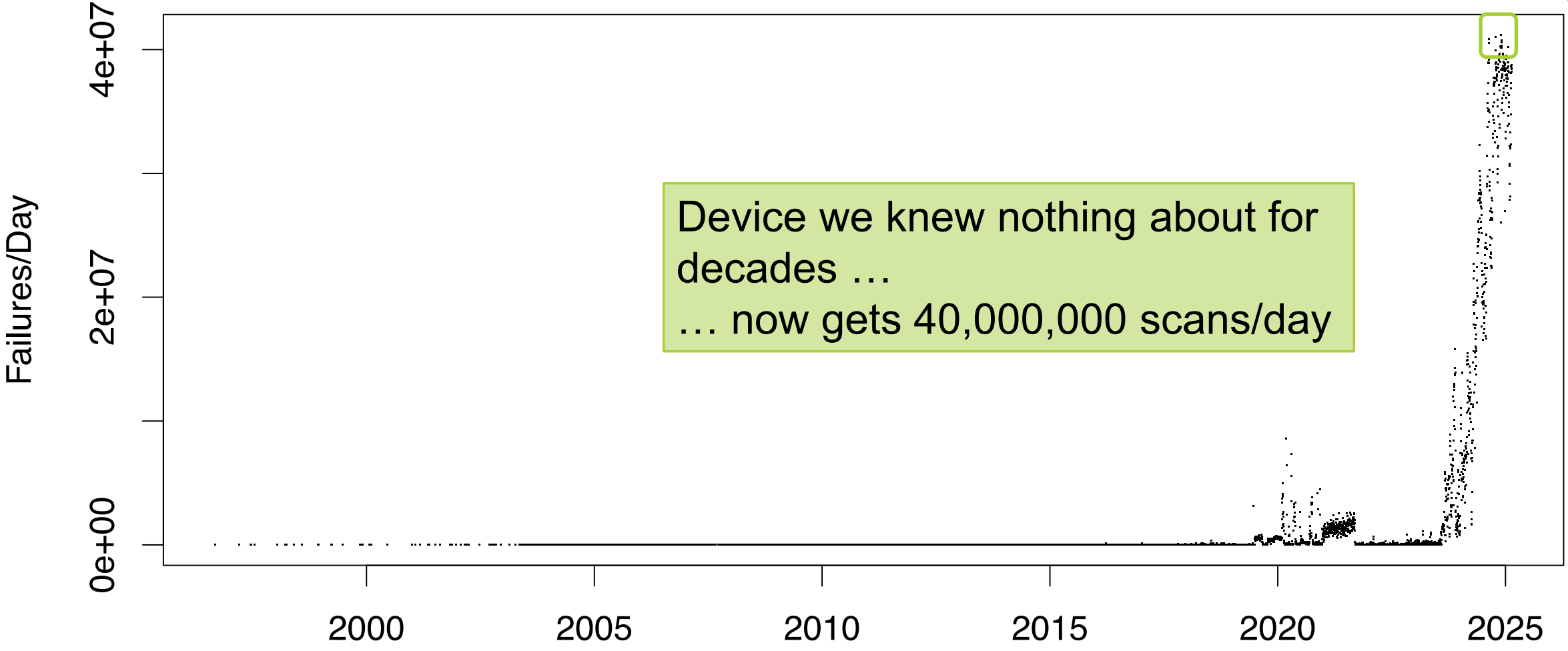
Network Management: SNMP



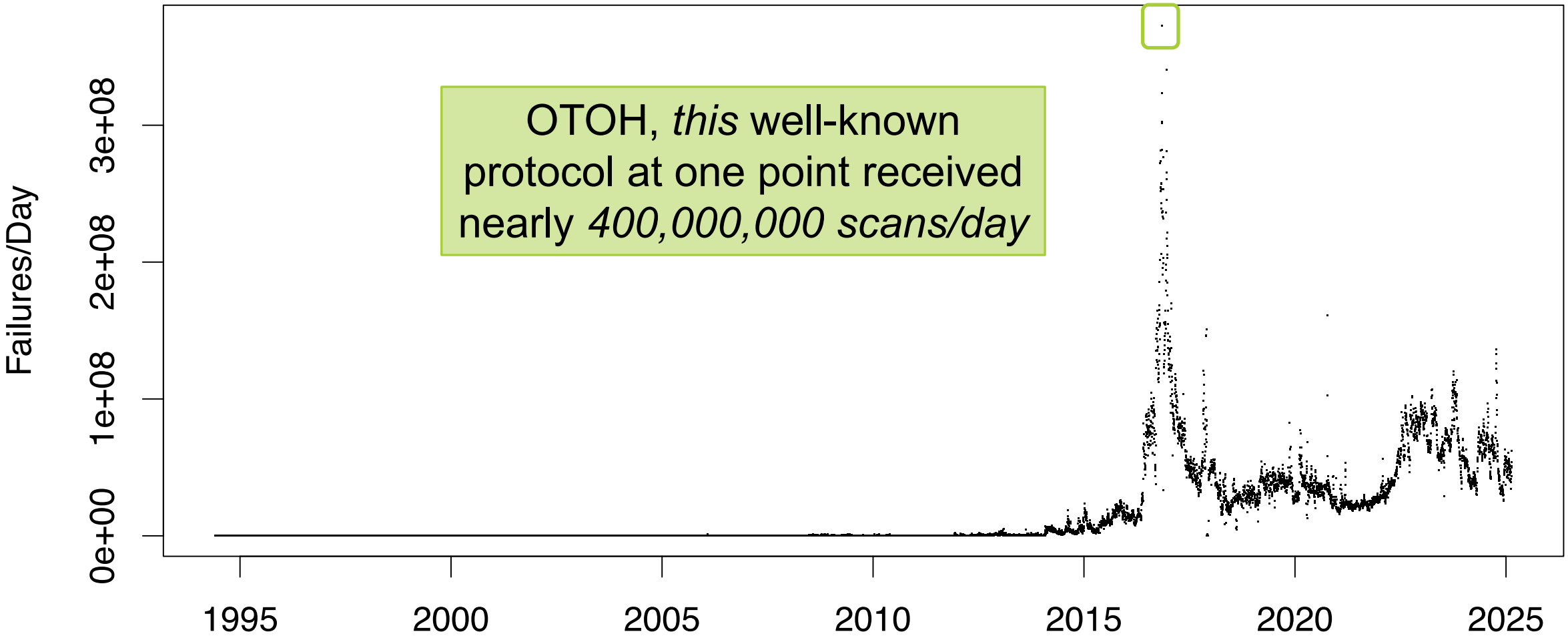
Unencrypted Remote Login: Shell



MikroTik Router API



Unencrypted Remote Login: Telnet



RSAC 2025 Conference

Decade #4 (2017-)

The Rise of Encryption

Many Voices.
One Community.

RSAC 2025 Conference

Decade #4 (2017-)

The Rise of Encryption?

Many Voices.
One Community.

RSAC 2025 Conference

Decade #4 (2017-)

*The Rise of Encryption?**

* From an enterprise perspective

Many Voices.
One Community.

RSAC 2025 Conference

Decade #4 (2017-)

*The Rise of Encryption?**

Part I: How Pervasive is QUIC?

Many Voices.
One Community.

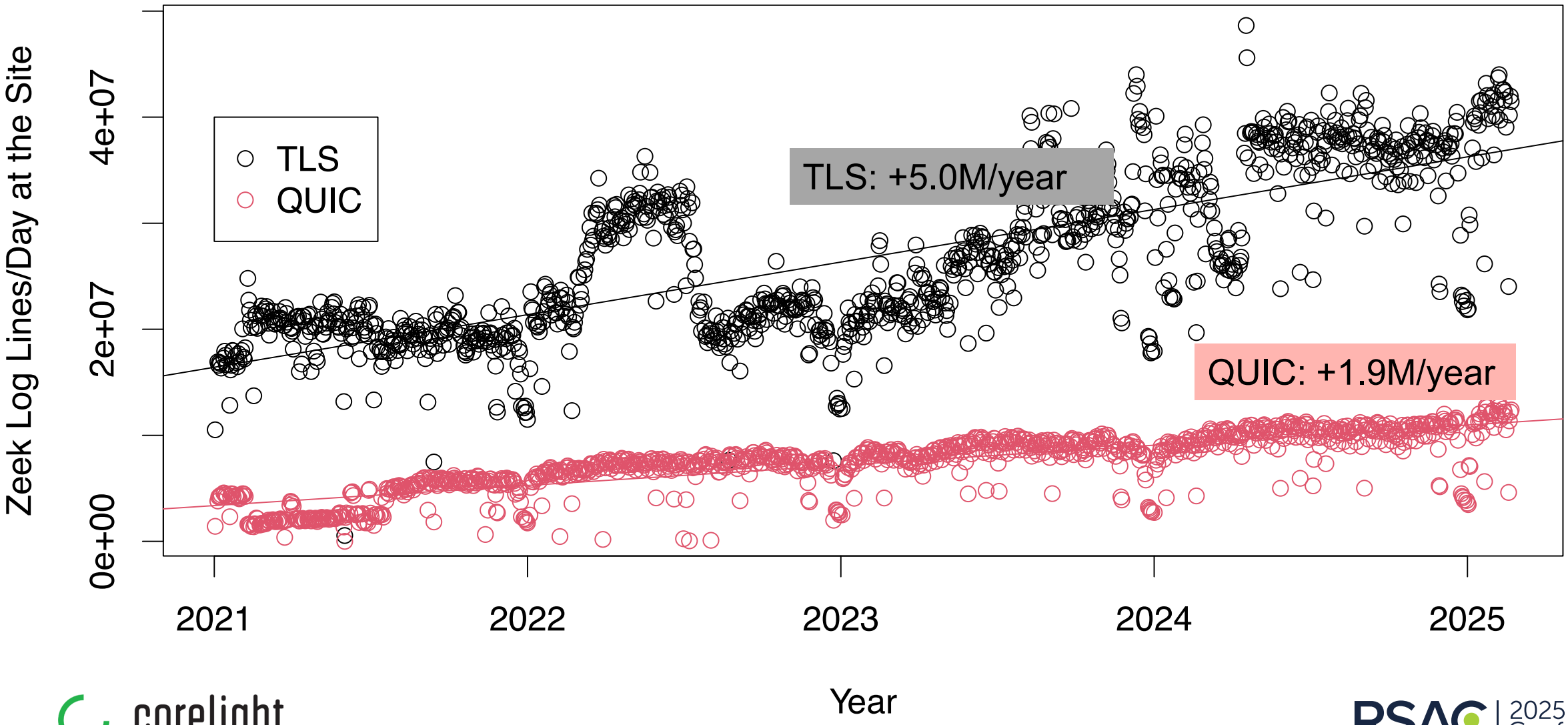
F5

PUBLISHED FEBRUARY 22, 2021

QUIC (not an acronym) is a unique beast, but is best thought of as a new transport protocol that solves many longstanding problems in the internet and captures most of the value provided by TCP, TLS, SCTP, IPSec, and HTTP/2. There is a new version of HTTP called HTTP/3 that is designed to work over UDP/QUIC instead of TCP/TLS.

Google deployed an early version of HTTP over QUIC in its browsers and web servers as early as 2014. An IETF standardization process began in 2016. After much evolution and data gathering, this will result in the first batch of RFCs in early 2021. Several major internet companies, including F5, have either shipped products that use QUIC or have deployed QUIC in their infrastructure. As of October 2020, 75% of Facebook's traffic was over HTTP/3 and QUIC.

Growth of TLS & QUIC Weekday Traffic



Proportion of *productive connections* as of late 2023

Site	IPv6 %	QUIC:TLS %
LBNL	62/2/0	23

RSAC 2025 Conference

Decade #4 (2017-)

*The Rise of Encryption?**

Part II:
How Pervasive is TLS 1.3?

Many Voices.
One Community.

* Hides certs; may hide SNI

Tracking the deployment of TLS 1.3 on the Web: A story of experimentation and centralization

Ralph Holz[1,2] , Jens Hiller[3] , Johanna Amann[4,2] , Abbas Razaghpanah[4] , Thomas Jost[3] , Narseo Vallina-Rodriguez[4,5] , Oliver Hohlfeld[6]
[1]University of Twente, [2]University of Sydney, [3]RWTH Aachen University, [4]ICSI, [5]IMDEA Networks, [6]Brandenburg University of Technology
r.holz@utwente.nl,{hiller,jost}@comsys.rwth-aachen.de,{johanna,abbas}@icir.org,narseo.vallina@imdea.org,hohlfeld@b-tu.de

ACM SIGCOMM Computer Communication Review

Volume 50 Issue 3, July 2020

For a profound view, we combine and analyze data from active domain scans, passive monitoring of large networks, and a crowd-sourcing effort on Android devices. In contrast to TLS 1.2, where adoption took more than five years and was prompted by severe attacks on previous versions, TLS 1.3 is deployed surprisingly speedily and without security concerns calling for it. Just 15 months after standardization, it is used in about 20% of connections we observe.

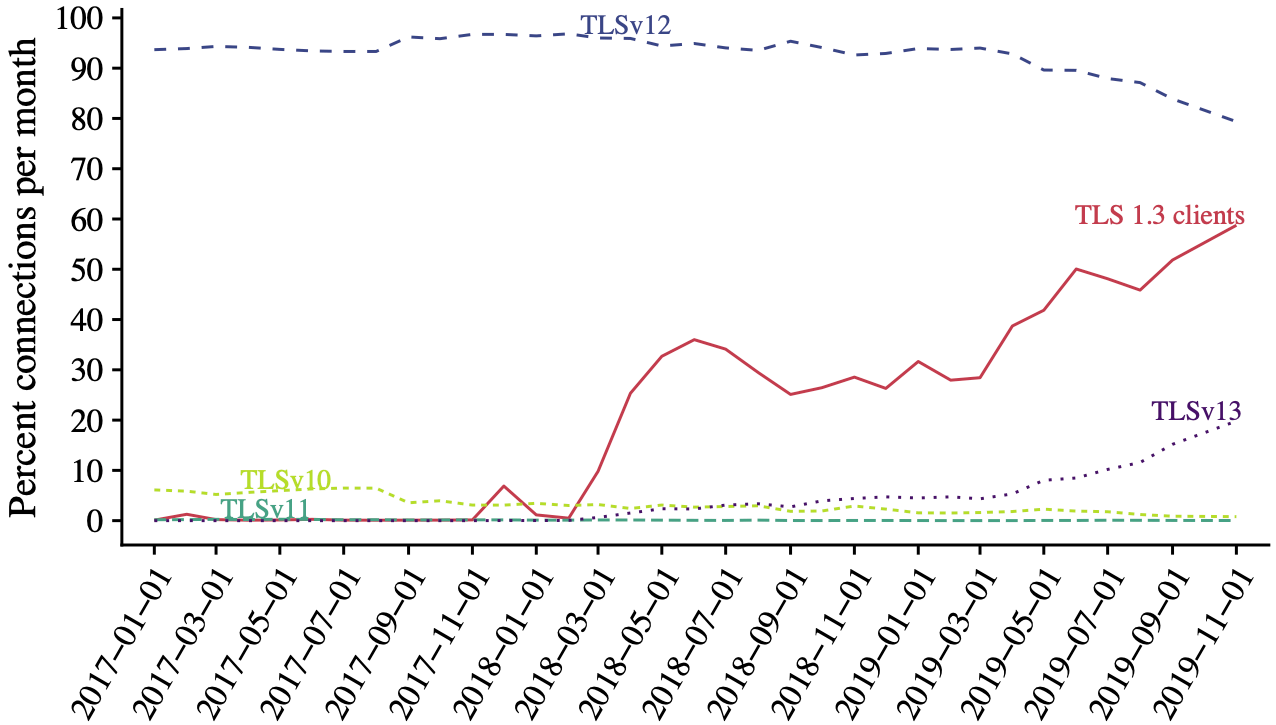
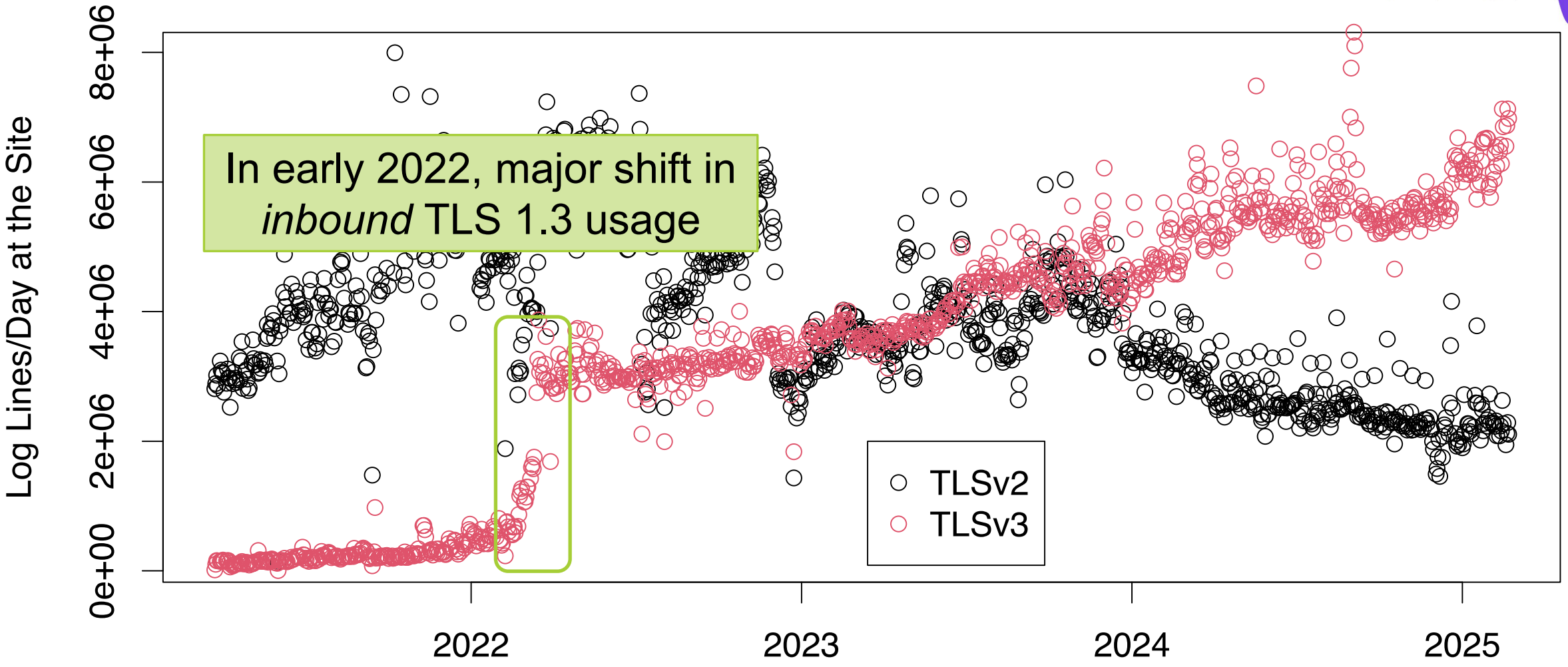
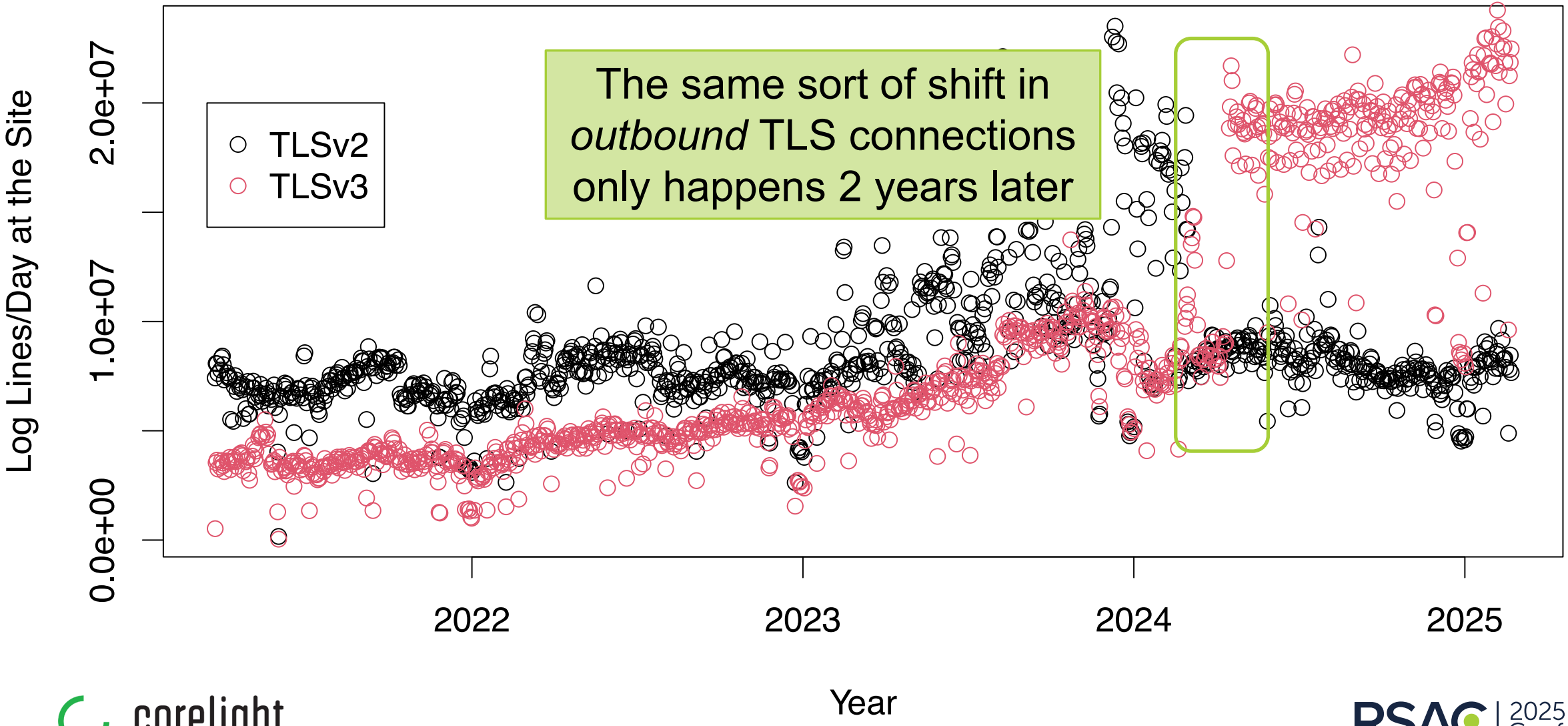


Figure 3: TLS 1.3 connections, view by Notary. Servers select TLS versions from client offers; clients offering TLS 1.3 in red.

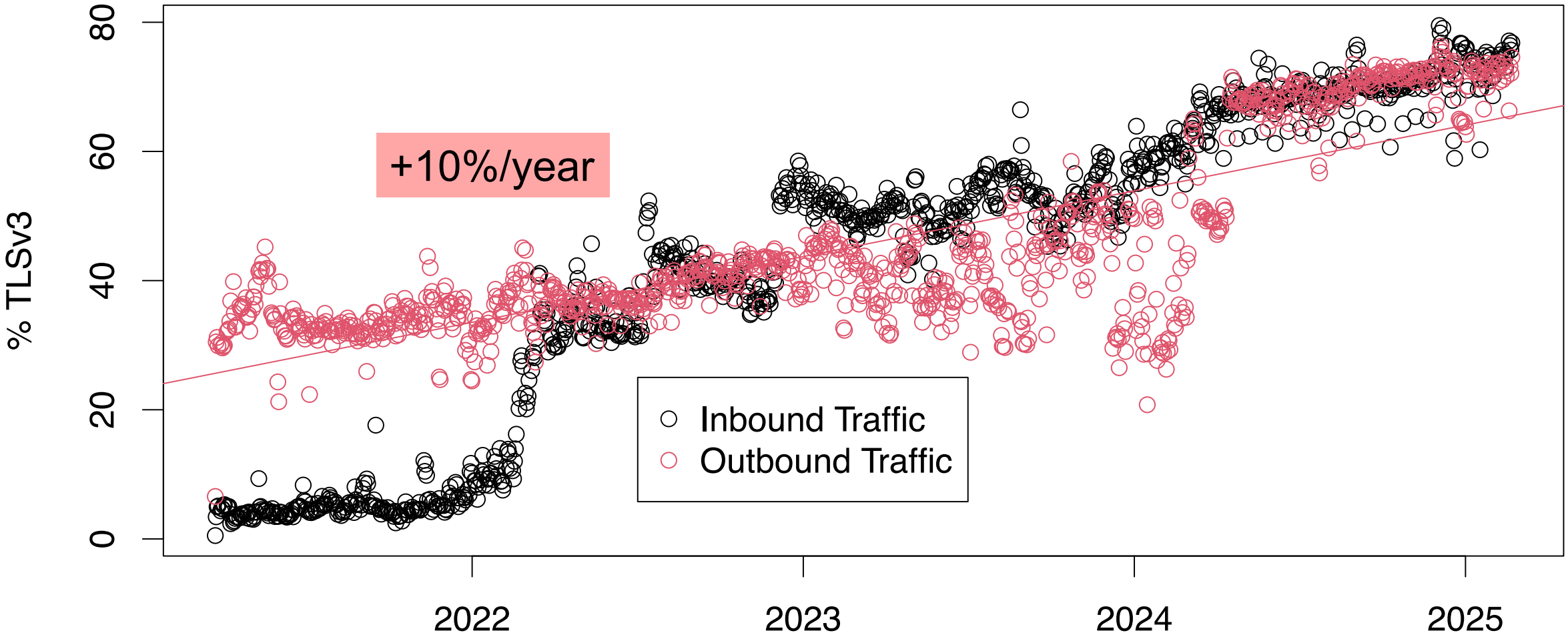
TLSv2 vs. TLSv3, Weekday Inbound Traffic



TLSv2 vs. TLSv3, Weekday Outbound Traffic



TLSv3:TLSv2 Ratio (Weekdays)



Proportion of *productive connections* as of late 2023

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %
LBNL	62/2/0	23	39

RSAC 2025 Conference

Decade #4 (2017-)

*The Rise of Encryption?**

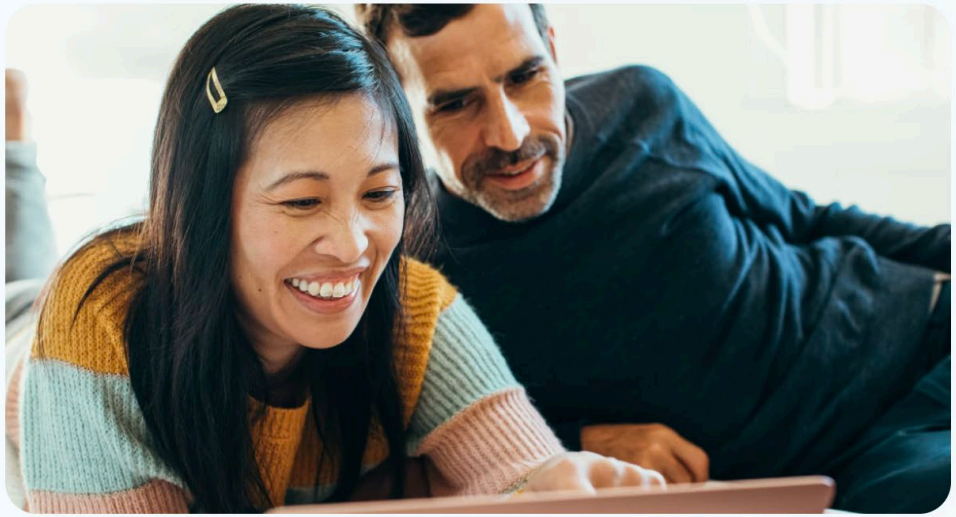
Part III: How Pervasive is SMBv3?

Many Voices.
One Community.

* Encrypted version of SMB

Microsoft | Windows Server Pricing Solutions Resources Try Windows Server

Blog home / Updates

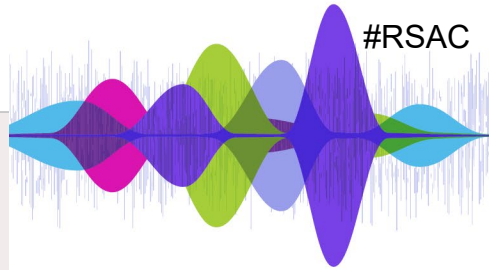


Updates · April 19, 2012 5 min read

SMB 2.2 is now SMB 3.0

By Jeffrey Snover

- **Secure data transfer with SMB encryption** – SMB Encryption protects data in-flight from eavesdropping and tampering attacks. Deployment is as simple as checking a box, with no additional setup requirements. This becomes more critical as mobile workers access data in centralized remote locations from unsecured networks. SMB Encryption is beneficial even within a secured corporate network if the data being accessed is sensitive..



Stop using SMB1

By Ned Pyle

Published Apr 10 2019 04:21 AM 705K Views

First published on TECHNET on Sep 16, 2016

Hi folks, Ned here again and today's topic is short and sweet:
Stop using SMB1. *Stop using SMB1* . ***STOP USING SMB1!***

In September of 2016, MS16-114 , a security update that prevents denial of service and remote code execution. If you need this security patch, you already have a much bigger problem: you are still running SMB1.

The original SMB1 protocol is nearly 30 years old , and like much of the software made in the 80's, it was designed for a world that no longer exists. A world without malicious actors, without vast sets of important data, without near-universal computer usage. Frankly, its naivete is staggering when viewed though modern eyes. I blame the West Coast hippy lifestyle :).

Proportion of *productive connections* as of late 2023

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	SMBv3? %
LBNL	62/2/0	23	39	

Proportion of *productive connections* as of late 2023

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	SMBv3 %
LBNL	62/2/0	23	39	0

Proportion of *productive connections* as of late 2023

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	SMBv3 %
LBNL	62/2/0	23	39	0*

* No SMBv3, but SMBv1 seen

RSAC 2025 Conference

Decade #4 (2017-)

Okay But That's Just One Datapoint, Right?

Many Voices.
One Community.

Corelight Labs

Polaris Program

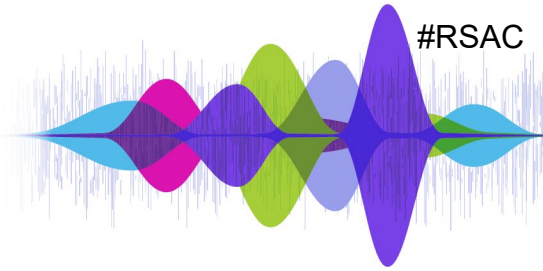
10 Polaris partners, 16 sensors deployed
17 billion Zeek logs/day
2+ PB stored pcaps

There is no substitute for access to extensive operational traffic. That's why the Polaris Program was created, and why it's vital to our research. Polaris is a partnership between Corelight and a select few of our customers that allows us to tap into the complexity of modern enterprise networks — vastly exceeding what's available in simulations or lab setups.

Polaris partners grant Corelight research access to their operational networks, and in return, receive expert attention to their networks via ongoing interactions with our research team and early access to the new capabilities we develop.

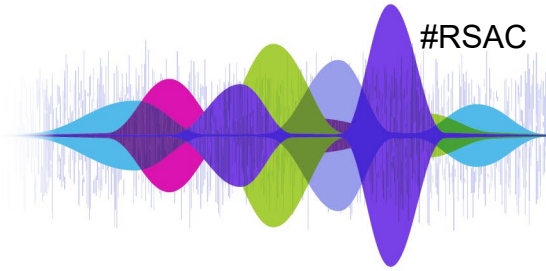
corelight

Per-Site Profile, Aug 2023



Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	SMBv3 %
LBNL	62/2/0	23	39	0

Per-Site Profile, Aug 2023



Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	SMBv3 %
LBNL	62/2/0	23	39	0
Polaris A	0	10	36	N/A
Polaris B	0	11	26	N/A
Polaris C	2	11	27	N/A
Polaris D	*none*	0	20	N/A
Polaris E	*none*	*none*	2	*none*
Polaris F	*none*	*none*	5	*none*
Polaris G	0	*none*	13	*none*
Polaris H	2	1	26	N/A
Polaris I	*none*	0	12	2

Per-Site Profile, Aug 2023

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	62/2/0	23	39		0	
Polaris A	0	10	36		N/A	N/A
Polaris B	0	11	26		N/A	N/A
Polaris C	2	11	27		N/A	N/A
Polaris D	*none*	0	20		N/A	N/A
Polaris E	*none*	*none*	2		*none*	
Polaris F	*none*	*none*	5		*none*	
Polaris G	0	*none*	13		*none*	
Polaris H	2	1	26		N/A	N/A
Polaris I	*none*	0	12		2	

Per-Site Profile, Aug 2023

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	62/2/0	23	39	✔	0	✔
Polaris A	0	10	36	✔	N/A	N/A
Polaris B	0	11	26	✔	N/A	N/A
Polaris C	2	11	27	✔	N/A	N/A
Polaris D	*none*	0	20	✔	N/A	N/A
Polaris E	*none*	*none*	2	✔	*none*	✔
Polaris F	*none*	*none*	5	✔	*none*	✔
Polaris G	0	*none*	13	✔	*none*	✔
Polaris H	2	1	26	✔	N/A	N/A
Polaris I	*none*	0	12	✔	2	✔

RSAC 2025 Conference

Decade #4 (2017-)

What's Changed Over the Last 18 Months?

Many Voices.
One Community.

Per-Site Profile, Feb 2025

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	46/5/3	28	72	✔	*none*	✔
Polaris A	0	24	75†	✔	3	✔
Polaris B	0	5	49	✔	0	✔
Polaris C	0	40	65†	✔	13	
Polaris D	*none*	0	37	✔	*none*	
Polaris E	*none*	1	19†	✔	*none*	✔
Polaris F	*none*	1	45	✔	*none*	✔
Polaris G	0	1	21†	✔	*none*	✔
Polaris H*	1	4	35	✔	*none*	✔
Polaris I	*none*	0	31†	✔	2	✔
Polaris J	37/12/12	3	64	✔	3	

Per-Site Profile, Feb 2025

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	46/5/3	28	72	✓	*none*	✓
Polaris A	0	24	75†	✓	3	✓
Polaris B	0	5	49	✓	0	✓
Polaris C	0	40	65†	✓	13	
Polaris D	*none*	0	37	✓	*none*	
Polaris E	*none*	1	19†	✓	*none*	✓
Polaris F	*none*	1	45	✓	*none*	✓
Polaris G	0	1	21†	✓	*none*	✓
Polaris H*	1	4	35	✓	*none*	✓
(data from Aug 2024)		0	31†	✓	2	✓
Polaris J	37/12/12	3	64	✓	3	

Per-Site Profile, Feb 2025

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	46/5/3	28	72	✓	*none*	✓
Polaris A	0	24	75	✓	3	✓
Polaris B	0	5	49	✓	0	✓
Polaris C	0	40	65	✓	13	
Polaris D	*none*	0	37	✓	*none*	
Polaris E	*none*	1	19	✓	*none*	✓
Polaris F	*none*	1	45	✓	*none*	✓
Polaris G	0	1	21	✓	*none*	✓
Polaris H*	1			✓	*none*	✓
Polaris I	*none*	0	31	✓	2	✓
Polaris J	37/12/12	3	64	✓	3	

Additional Polaris site

Changes Aug 2023 ⟶ Feb 2025

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	46/5/3	28	72	✔	*none*	✔
Polaris A	0	24	75†	✔	3	✔
Polaris B	0	5	49	✔	0	✔
Polaris C	0			✔	13	
Polaris D	*none*			✔	*none*	
Polaris E	*none*			✔	*none*	✔
Polaris F	*none*	1	45	✔	*none*	✔
Polaris G	0	1	21†	✔	*none*	✔
Polaris H*	1	4	35	✔	*none*	✔
Polaris I	*none*	0	31†	✔	2	✔
Polaris J	37/12/12	3	64	✔	3	

These all actually went **down**

Changes Aug 2023 ⟶ Feb 2025

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	46/5/3	28	72	✓	*none*	✓
Polaris A	0	24	75	✓	3	✓
Polaris B	0	5	49	✓	0	✓
Polaris C	0	40	65	✓	13	
Polaris D	*none*	0			*none*	
Polaris E	*none*	1		✓	*none*	✓
Polaris F	*none*	1	45	✓	*none*	✓
Polaris G	0	1	21	✓	*none*	✓
Polaris H*	1	4	35	✓	*none*	✓
Polaris I	*none*	0	31	✓	2	✓
Polaris J	37/12/12	3	64	✓	3	

Only significant at 3 sites;
B fell by 2x

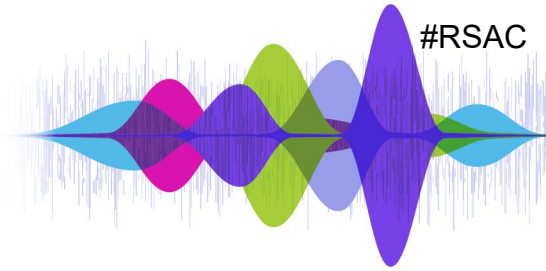
Changes Aug 2023 ⟶ Feb 2025

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	46/5/3	28	72	✓	*none*	✓
Polaris A	0	24	75†	✓	3	✓
Polaris B	0	5	49	✓	0	✓
Polaris C	0	40	65†	✓	13	
Polaris D	*none*	0	37			
Polaris E	*none*	1	19†			
Polaris F	*none*	1	45	✓	*none*	✓
Polaris G	0	1	21†	✓	*none*	✓
Polaris H*	1	4	35	✓	*none*	✓
Polaris I	*none*	0	31†	✓	2	✓
Polaris J	37/12/12	3	64	✓	3	

Grew significantly at every site;
But still not predominant at most sites

Changes Aug 2023 ⟶ Feb 2025

Site	IPv6 %	QUIC:TLS %	TLS 1.3:TLS %	TLS 1.0 in use?	SMBv3 %	SMBv1 in use?
LBNL	46/5/3	28	72	✔	*none*	✔
Polaris A	0	24	75†	✔	3	✔
Polaris B	0	5	49	✔	0	✔
Polaris C	0	40	65†		13	
Polaris D	*none*	0	37	'nuf said	*none*	
Polaris E	*none*	1	19†	✔	*none*	✔
Polaris F	*none*	1	45	✔	*none*	✔
Polaris G	0	1	21†	✔	*none*	✔
Polaris H*	1	4	35	✔	*none*	✔
Polaris I	*none*	0	31†	✔	2	✔
Polaris J	37/12/12	3	64	✔	3	



AWS Security Blog

Post-quantum TLS now supported in AWS KMS

by Andrew Hopkins | on 04 NOV 2019 | in Advanced (300), AWS Key Management Service, Security, Identity, & Compliance | Permalink | Comments | Share

AWS Key Management Service (AWS KMS) now supports post-quantum hybrid key exchange for the Transport Layer Security (TLS) network encryption protocol that is used when connecting to KMS API endpoints. In this post, I'll tell you what post-quantum TLS is, what hybrid key exchange is, why it's important, how to take advantage of this new feature, and how to give us feedback.

What is post-quantum TLS?

Post-quantum TLS is a feature that adds new, post-quantum cipher suites to the protocol. AWS implements TLS using s2n, a streamlined open source implementation of TLS. In June, 2019, AWS introduced post-quantum s2n, which implements two proposed post-quantum hybrid cipher suites specified in this IETF draft. The cipher suites specify a key exchange that provides the security protections of both the classical and post-quantum schemes.

Why is this important?

A large-scale quantum computer would break the current public key cryptography that is used for key exchange in every

AWS Security Blog

Post-quantum TLS now supported in AWS KMS

by Andrew Hopkins | on 04 NOV 2019 | in Advanced (300), AWS Key Management Service
Compliance | Permalink | Comments | Share

AWS Key Management Service (AWS KMS) now supports post-quantum hybrid key exchange fo
Security (TLS) network encryption protocol that is used when connecting to KMS API endpoints
what post-quantum TLS is, what hybrid key exchange is, why it's important, how to take advant
and how to give us feedback.

What is post-quantum TLS?

Post-quantum TLS is a feature that adds new, post-quantum cipher suites to the protocol. AWS implements TLS
s2n, a streamlined open source implementation of TLS. In June, 2019, AWS introduced post-quantum s2n, whic
implements two proposed post-quantum hybrid cipher suites specified in this IETF draft. The cipher suites speci
exchange that provides the security protections of both the classical and post-quantum schemes.

Why is this important?

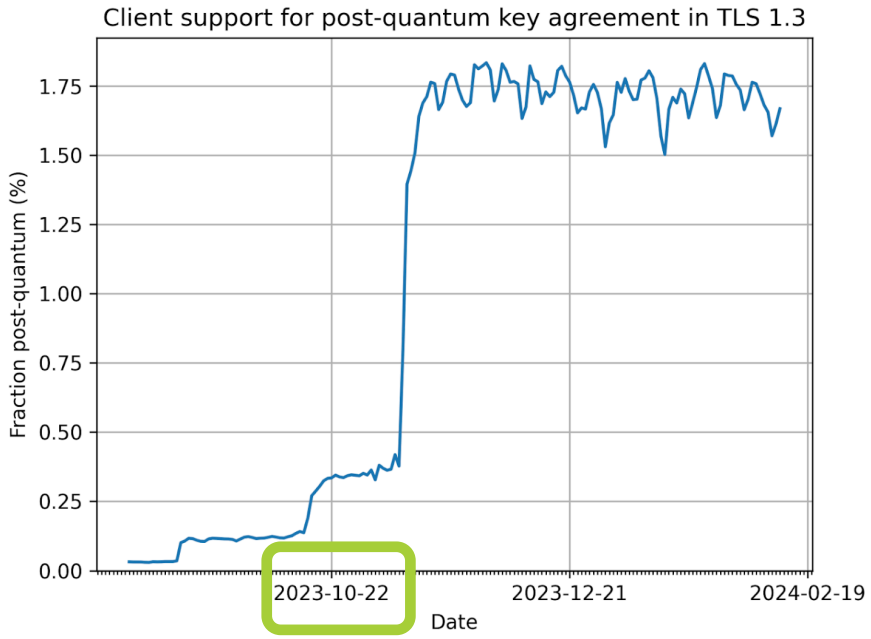
A large-scale quantum computer would break the current public key cryptography that is used for key exchange

CLOUDFLARE The Cloudflare Blog

The state of the post-quantum Internet

2024-03-05

Bas Westerbaan



Fraction of TLS 1.3 connections established with Cloudflare that are secured with post-quantum cryptography.

End of the road for RC4

2015-02-23

John Graham-Cumming

Today, we completely disabled the RC4 encryption algorithm for all SSL/TLS connections to CloudFlare sites. It's no longer possible to connect to any site that uses CloudFlare using RC4.

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Disabling SSLv3 and RC4

September 17, 2015

Posted by Adam Langley, Security Engineer

As the previously announced transition to SHA-256 certificates is nearing completion, we are planning the next changes to Google's TLS configuration. As part of those changes, we expect to disable support for SSLv3 and RC4 in the n

SSLv3 has been obsole

it must no longer be us

subject of multiple atta

statement that it too m

End of the road for RC4

2015-02-23

John Graham-Cumming

Today, we completely disabled the RC4 encryption algorithm for all SSL/TLS connections to CloudFlare sites. It's no longer possible to connect to any site that uses CloudFlare using RC4.

Support Disabled for SSLv3 and RC4 for Gmail SMTP/IMAP/POP

June 24, 2016

Effectiv June 16, 2016, Google has disabled support for two security systems called SSLv3 and RC4 support at Google's SMTP servers, IMAP/POP clients, and on Gmail's web servers for the following reasons:

- SSLv3 has been obsolete for over 16 years and the Internet Engineering Task Force (IETF) has decided it must no longer be used
- RC4 is a 28-year old cipher that is now the subject of multiple attacks at security conferences. The IETF has decided that RC4 also must no longer be used

Per-Site Profile, Feb 2025

Site	IPv6 %	QUIC: TLS %	TLS 1.3: TLS %	TLS 1.0 ?	SMBv3 %	SMBv1 ?	Post-Quantum ?	RC4?
LBNL	46/5/3	28	72	✔	*none*	✔		
Polaris A	0	24	75	✔	3	✔		
Polaris B	0	5	49	✔	0	✔		
Polaris C	0	40	65	✔	13			
Polaris D	*none*	0	37	✔	*none*			
Polaris E	*none*	1	19	✔	*none*	✔		
Polaris F	*none*	1	45	✔	*none*	✔		
Polaris G	0	1	21	✔	*none*	✔		
Polaris H*	1	4	35	✔	*none*	✔		
Polaris I	*none*	0	31	✔	2	✔		
Polaris J	37/12/12	3	64	✔	3			

Per-Site Profile, Feb 2025

Site	IPv6 %	QUIC: TLS %	TLS 1.3: TLS %	TLS 1.0 ?	SMBv3 %	SMBv1 ?	Post-Quantum ?	RC4?
LBNL	46/5/3	28	72	✔	*none*	✔		
Polaris A	0	24	75	✔	3	✔		
Polaris B	0	5	49	✔	0	✔		
Polaris C	0	40	65	✔				
Polaris D	*none*	0	37	✔				
Polaris E	*none*	1	19	✔		✔		
Polaris F	*none*	1	45	✔	*none*	✔		
Polaris G	0	1	21	✔	*none*	✔		
Polaris H*	1	4	35	✔	*none*	✔		
Polaris I	*none*	0	31	✔	2	✔		
Polaris J	37/12/12	3	64	✔	3			

Would be good to see this …

Per-Site Profile, Feb 2025

Site	IPv6 %	QUIC: TLS %	TLS 1.3: TLS %	TLS 1.0 ?	SMBv3 %	SMBv1 ?	Post-Quantum ?	RC4?
LBNL	46/5/3	28	72	✔	*none*	✔		
Polaris A	0	24	75	✔	3	✔		
Polaris B	0	5	49	✔	0	✔		
Polaris C	0	40	65	✔				
Polaris D	*none*	0	37	✔				
Polaris E	*none*	1	19	✔		✔		
Polaris F	*none*	1	45	✔	*none*	✔		
Polaris G	0	1	21	✔	*none*	✔		
Polaris H*	1	4	35	✔	*none*	✔		
Polaris I	*none*	0	31	✔	2	✔		
Polaris J	37/12/12	3	64	✔	3			

… and *not* good to see this

Per-Site Profile, Feb 2025

Site	IPv6 %	QUIC: TLS %	TLS 1.3: TLS %	TLS 1.0 ?	SMBv3 %	SMBv1 ?	Post-Quantum ?	RC4?
LBNL	46/5/3	28	72	✓	*none*	✓	68	✓
Polaris A	0	24	75	✓	3	✓	4	
Polaris B	0	5	49	✓	0	✓		
Polaris C	0	40	65	✓	13		2	✓
Polaris D	*none*	0	37	✓	*none*		0	✓
Polaris E	*none*	1	19	✓	*none*	✓	0	✓
Polaris F	*none*	1	45	✓	*none*	✓	0	✓
Polaris G	0	1	21	✓	*none*	✓	*none*	✓
Polaris H*	1	4	35	✓	*none*	✓	0	
Polaris I	*none*	0	31	✓	2	✓	1	
Polaris J	37/12/12	3	64	✓	3		5	✓

Went from 0 to 39% in **one day**

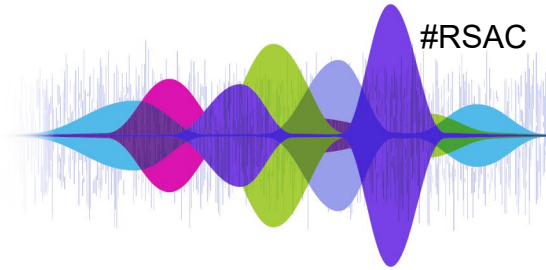
RSAC 2025 Conference

Decade #4 (2017-)

Okay But At Least Not Much Clear-Text HTTP, Right?

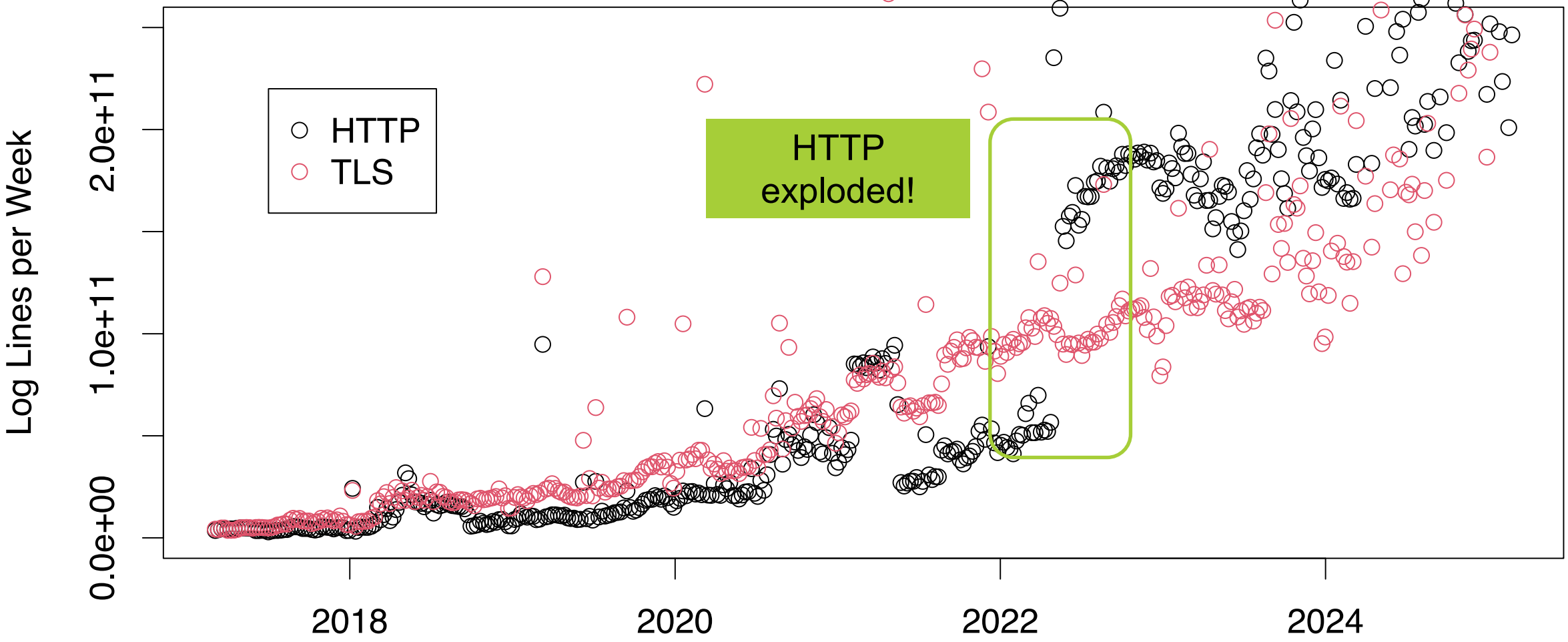
Many Voices.
One Community.

Telemetry from (**many**) online Corelight sensors

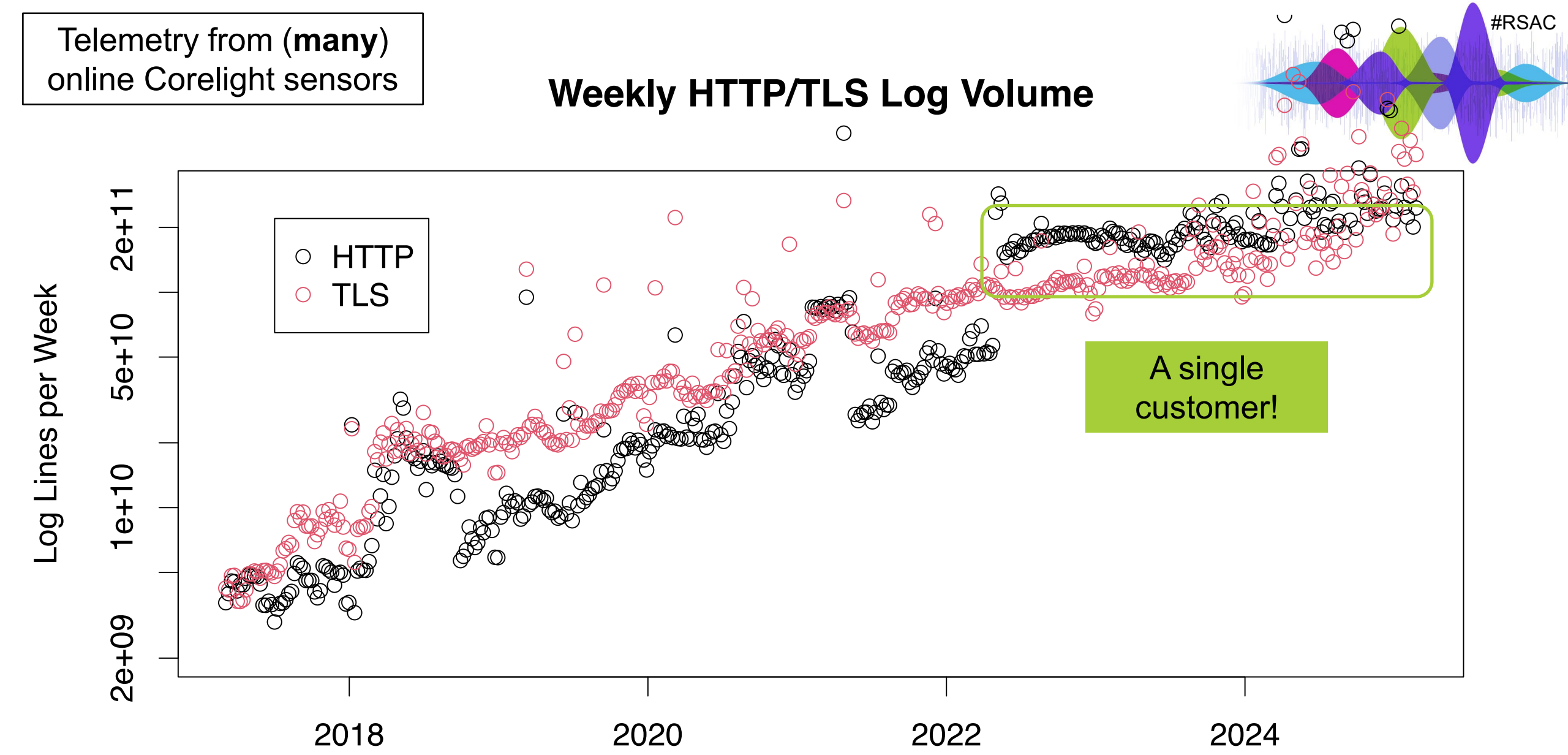


Telemetry from (**many**) online Corelight sensors

Weekly HTTP/TLS Log Volume

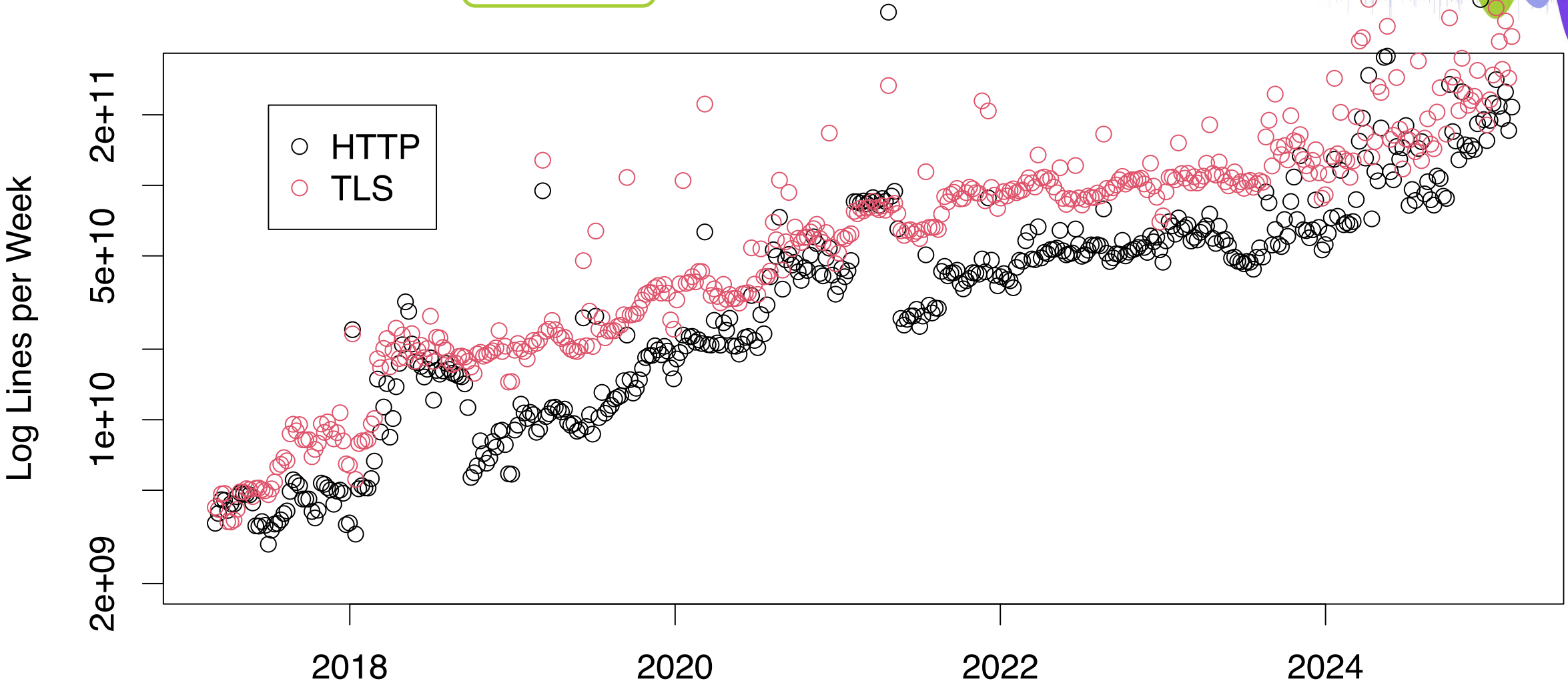


Telemetry from (**many**) online Corelight sensors



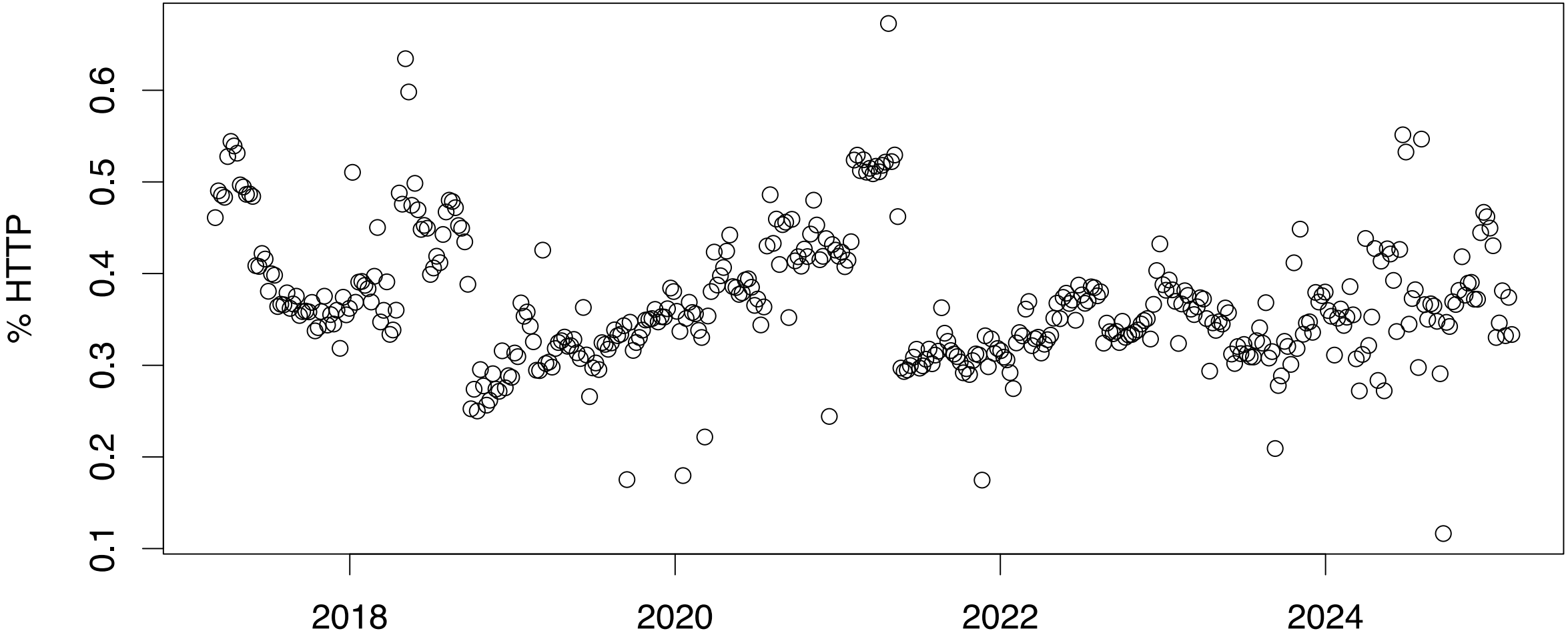
Telemetry from (**many**) online Corelight sensors

Adjusted Weekly HTTP/TLS Log Volume



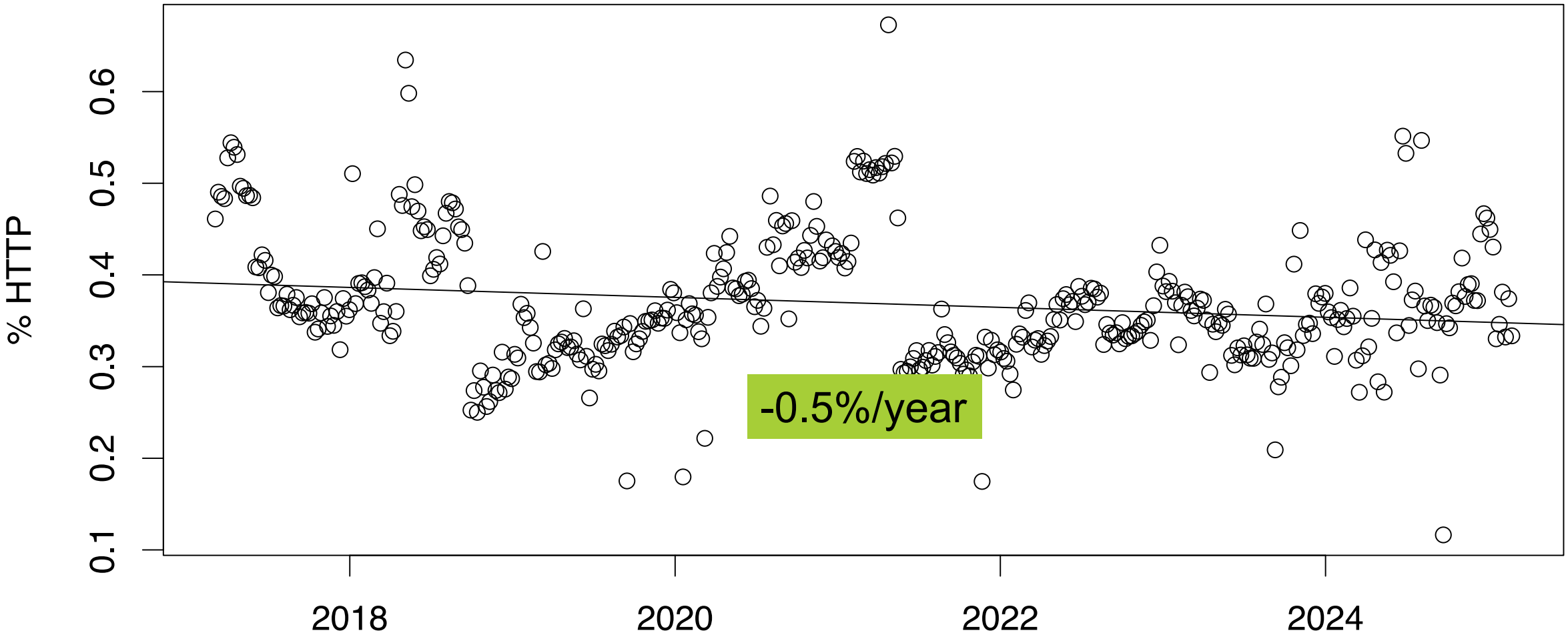
Telemetry from (**many**) online Corelight sensors

HTTP:TLS Ratio (Adjusted)



Telemetry from (**many**) online Corelight sensors

HTTP:TLS Ratio (Adjusted)



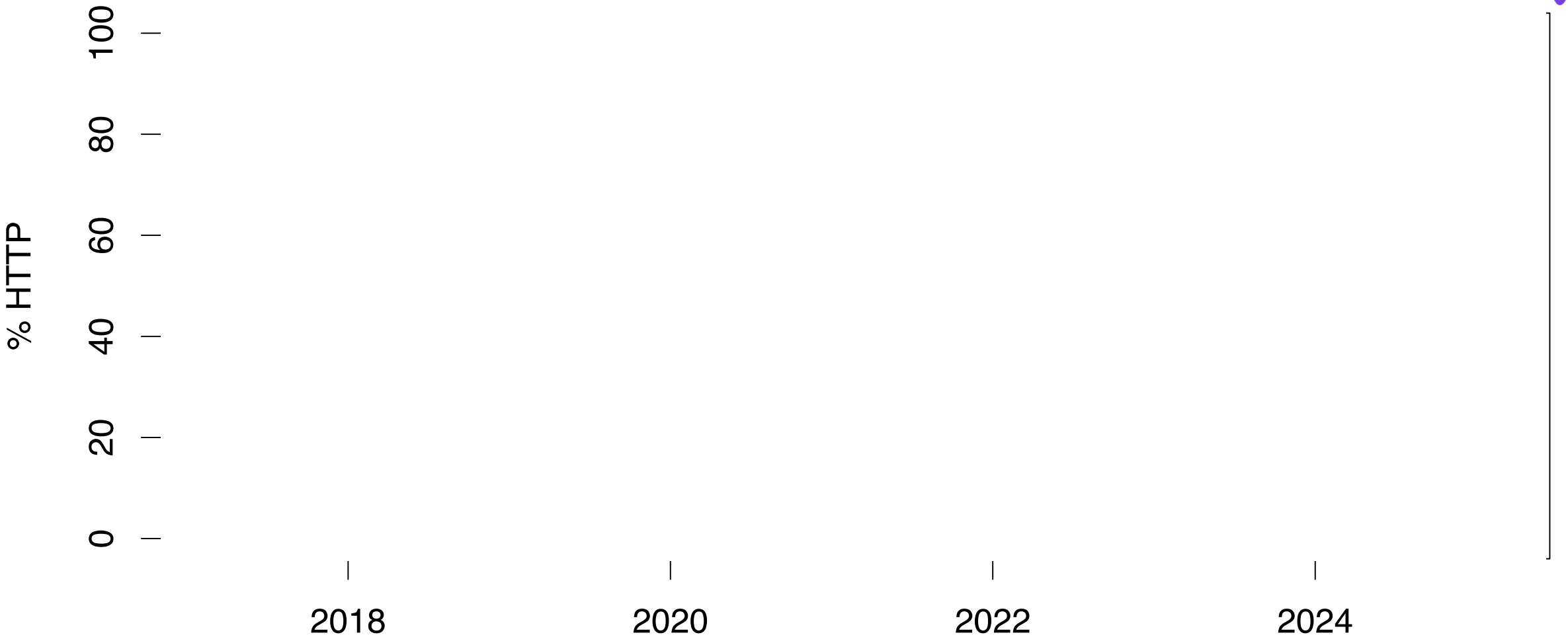
RSAC 2025 Conference

Decade #4 (2017-)

Okay But That's Just Dominated By A Few Big-and-Lax Weirdos, Right?

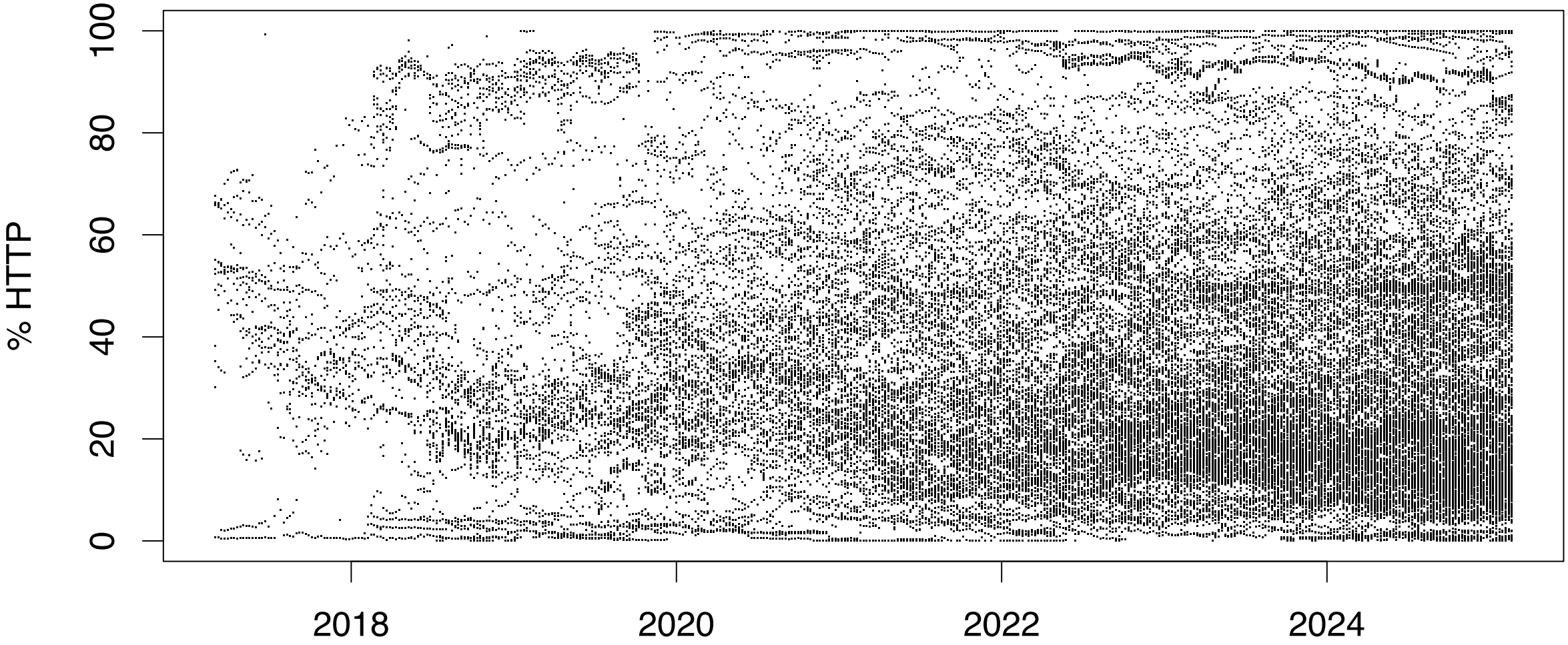
Many Voices.
One Community.

HTTP:(HTTP+TLS) Ratio for Individual Corelight Sensors



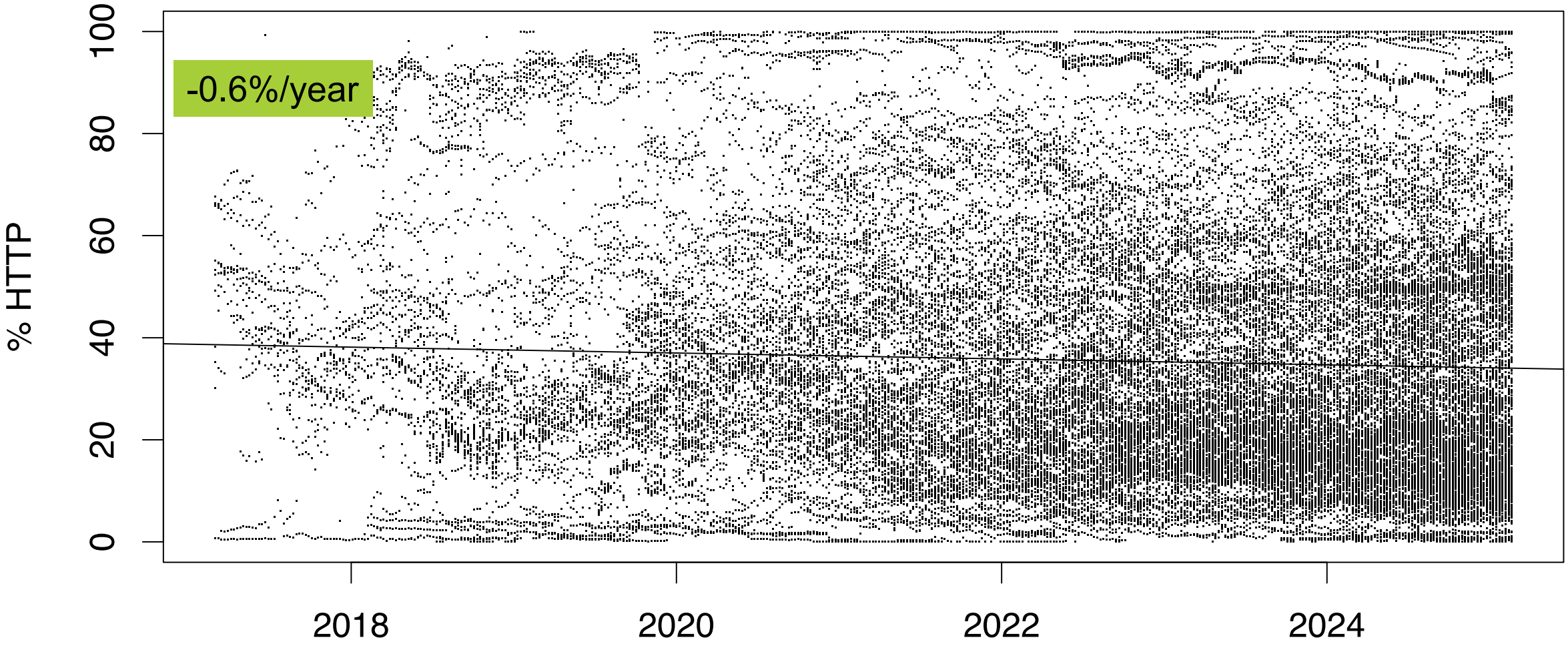
Each point represents one sensor, 100M+ combined logs/week

HTTP:(HTTP+TLS) Ratio for Individual Corelight Sensors



Each point represents one sensor, 100M+ combined logs/week

HTTP:(HTTP+TLS) Ratio for Individual Corelight Sensors



Each point represents one sensor, 100M+ combined logs/week

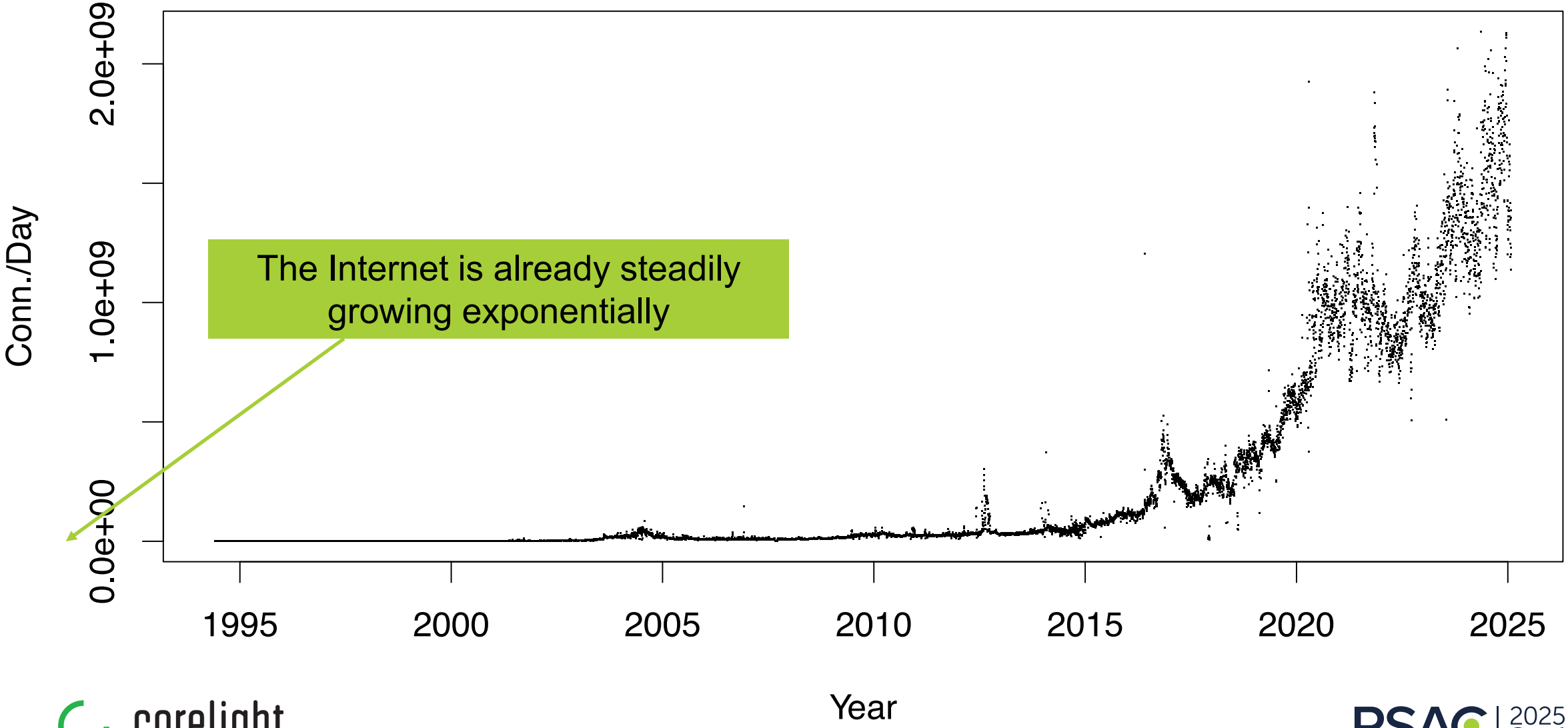
corelight

RSAC™ 2025 Conference

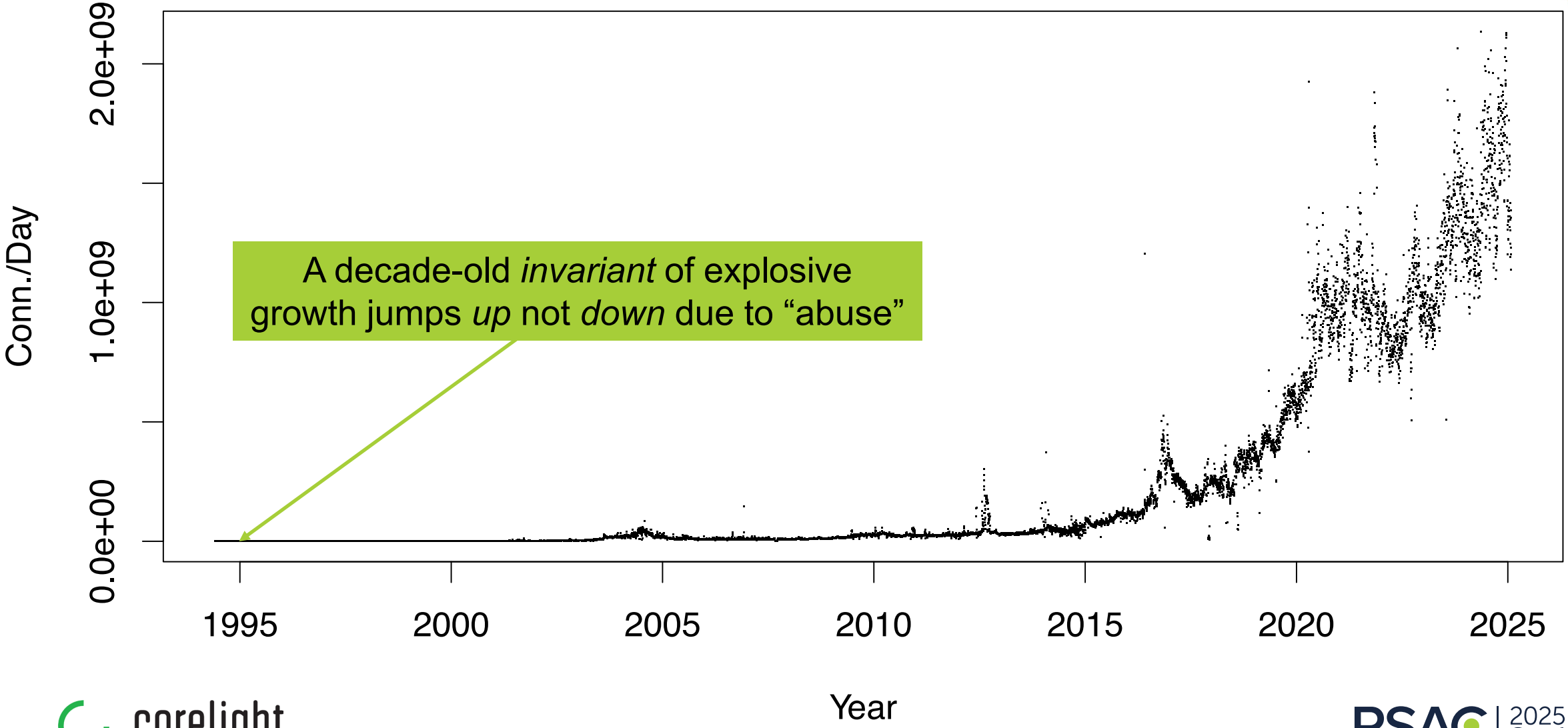
So What Have We Seen?

Many Voices.
One Community.

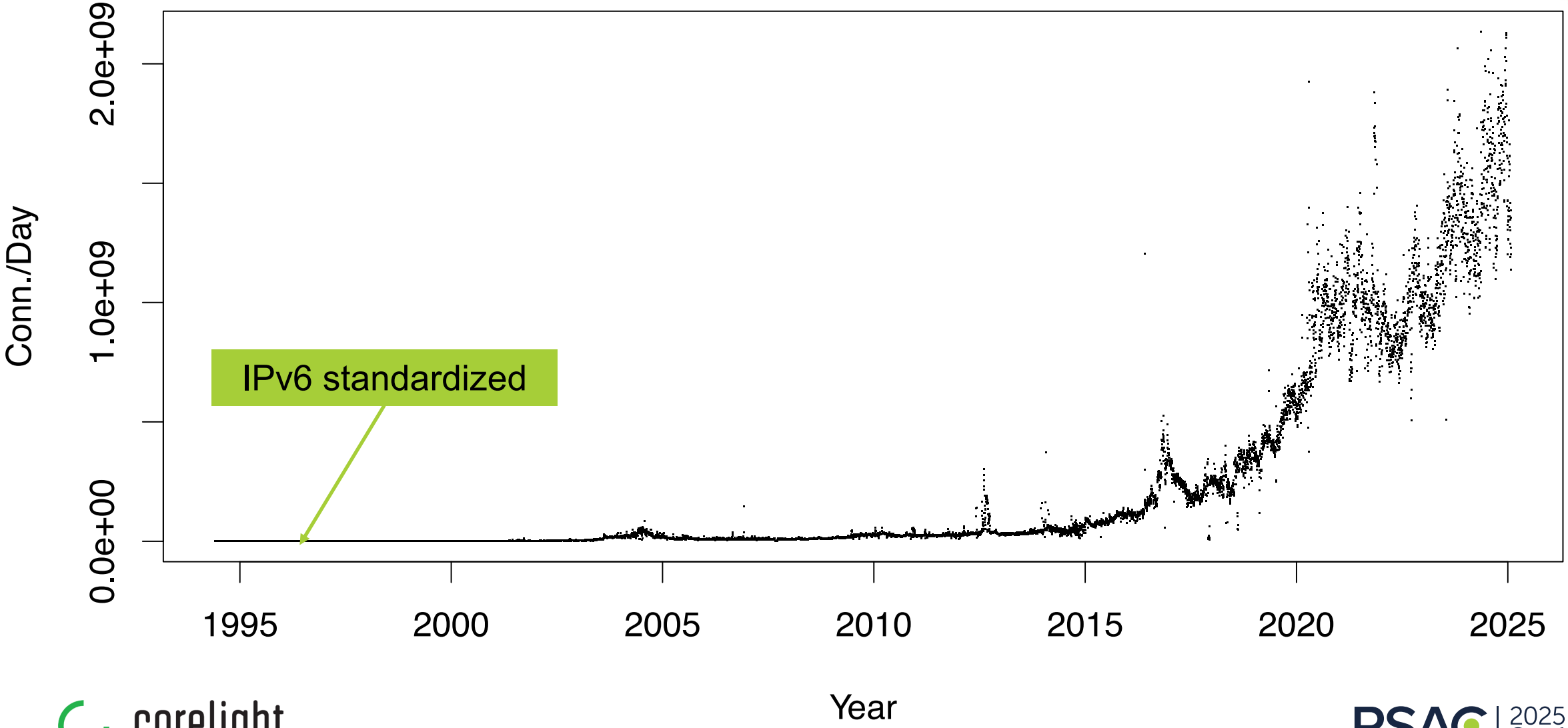
Evolution of Inbound Connections Per Day (LBNL)



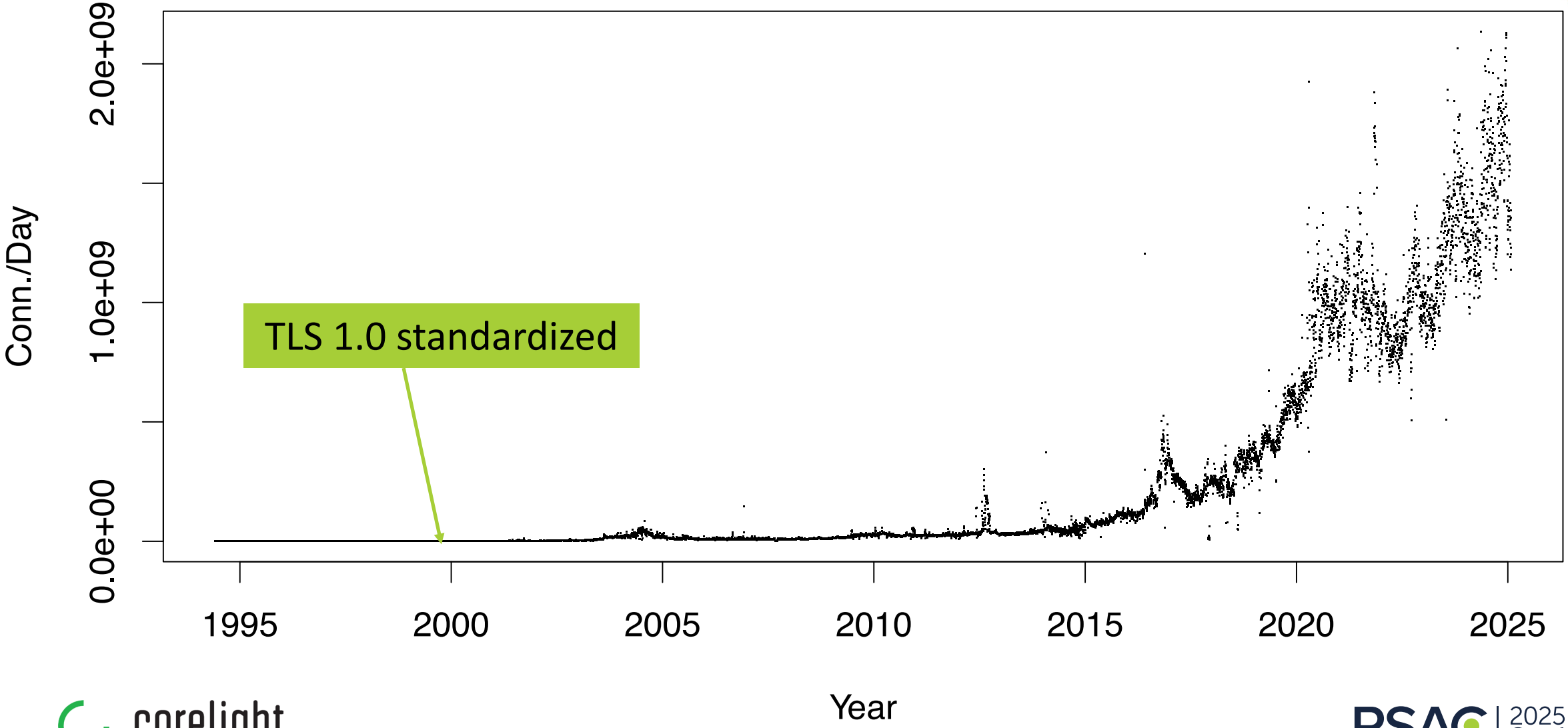
Evolution of Inbound Connections Per Day (LBNL)



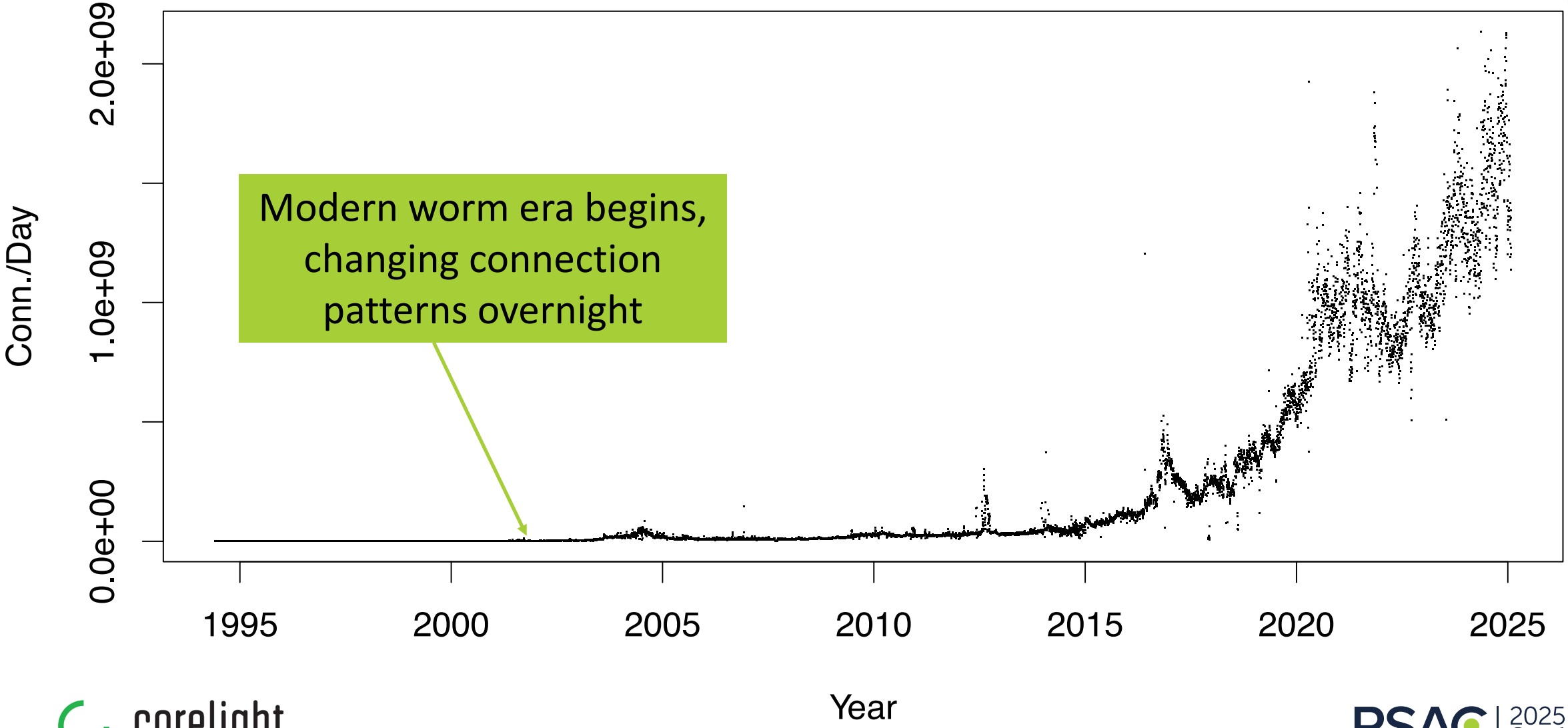
Evolution of Inbound Connections Per Day (LBNL)



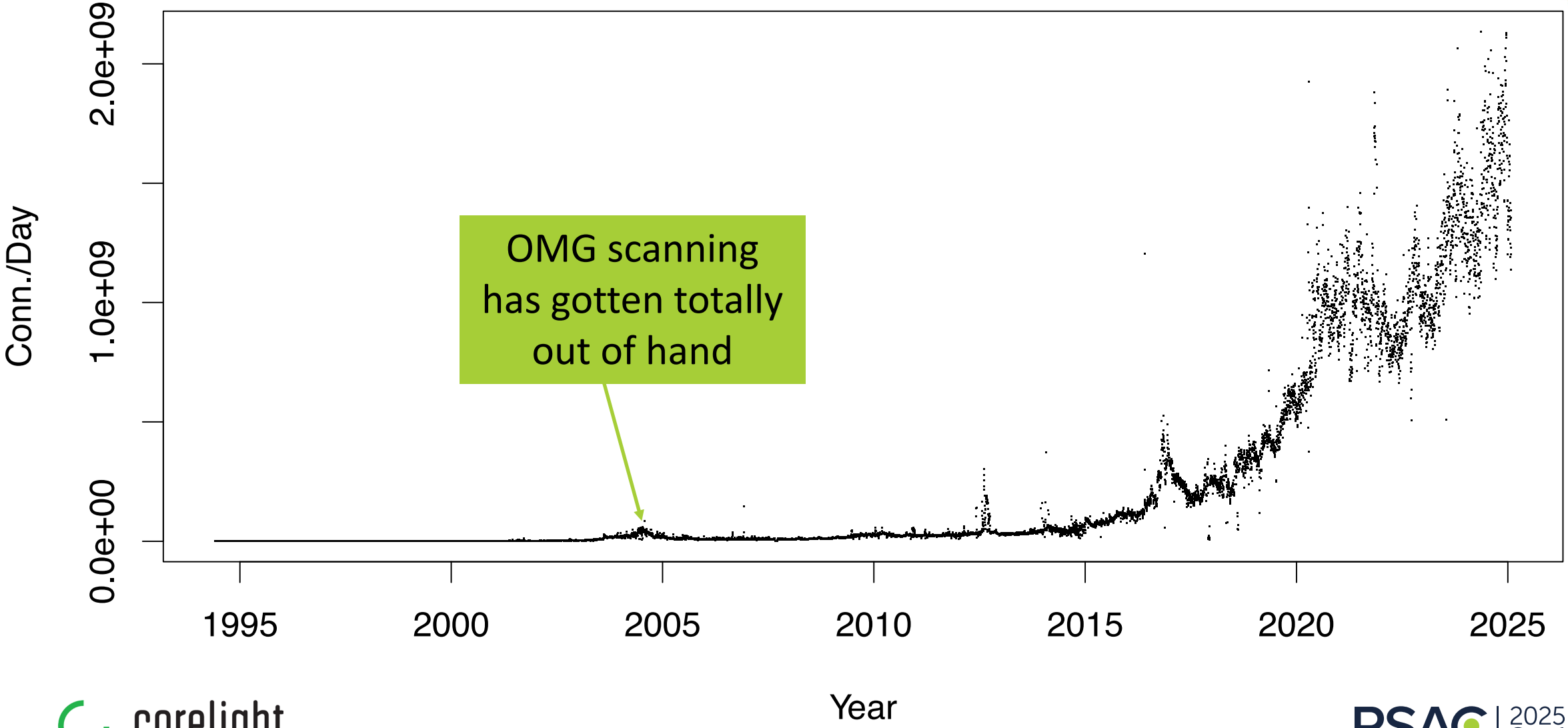
Evolution of Inbound Connections Per Day (LBNL)



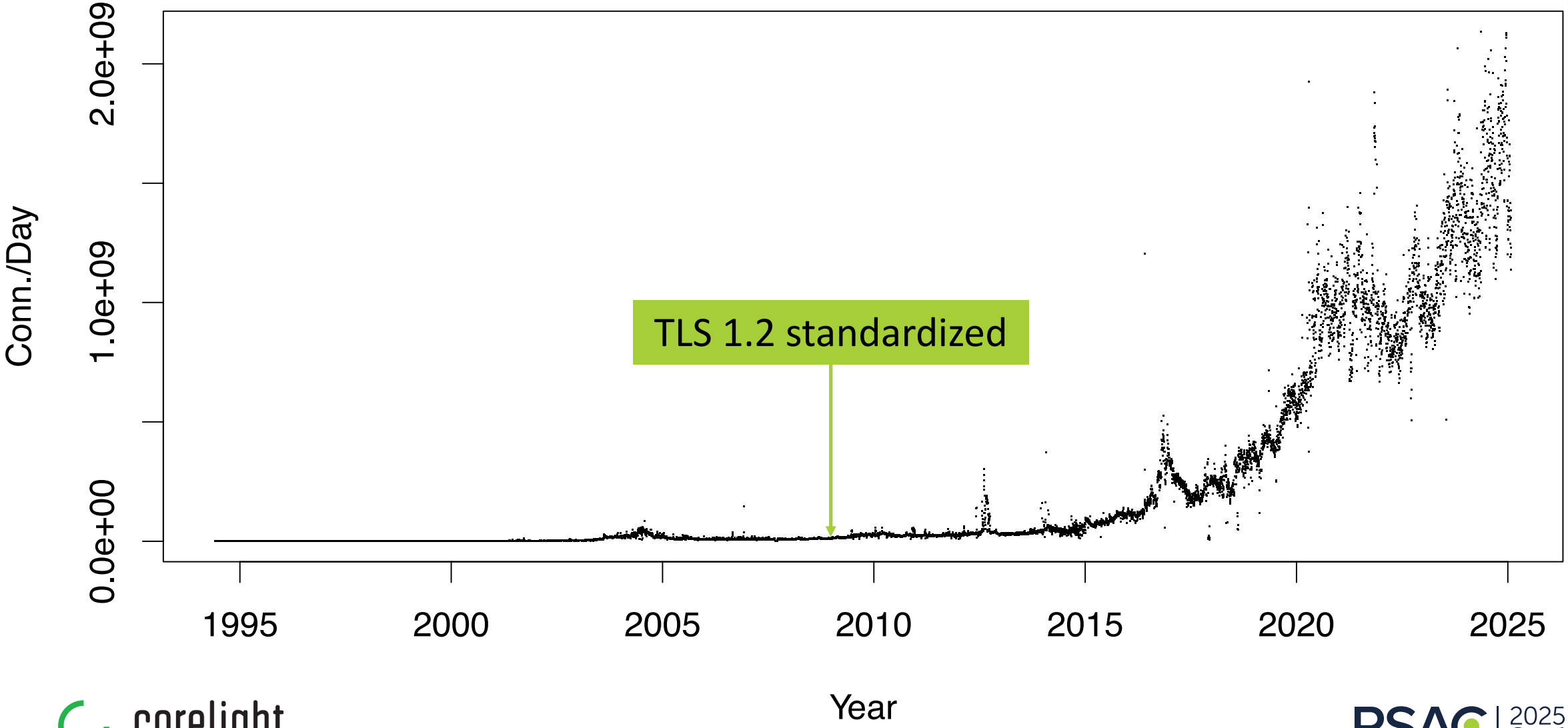
Evolution of Inbound Connections Per Day (LBNL)



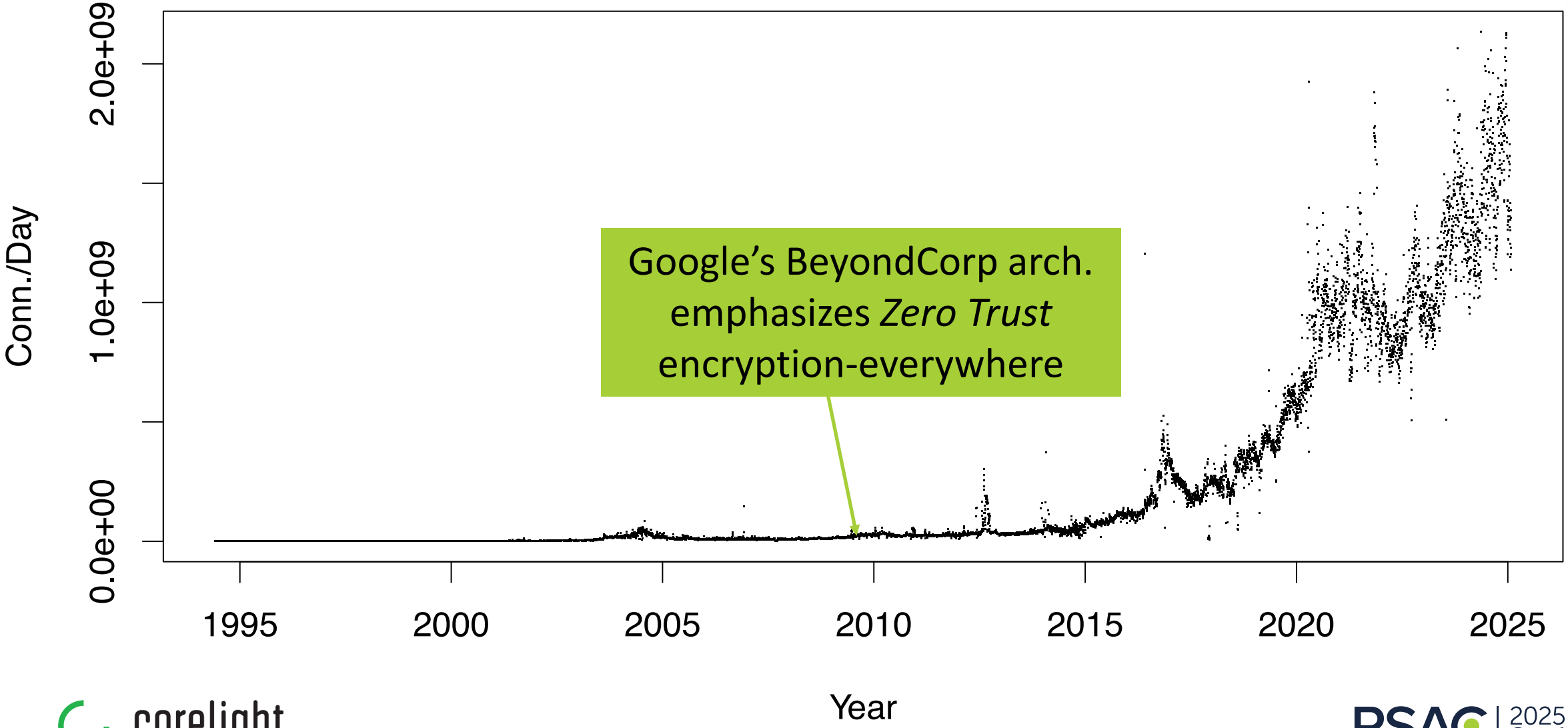
Evolution of Inbound Connections Per Day (LBNL)



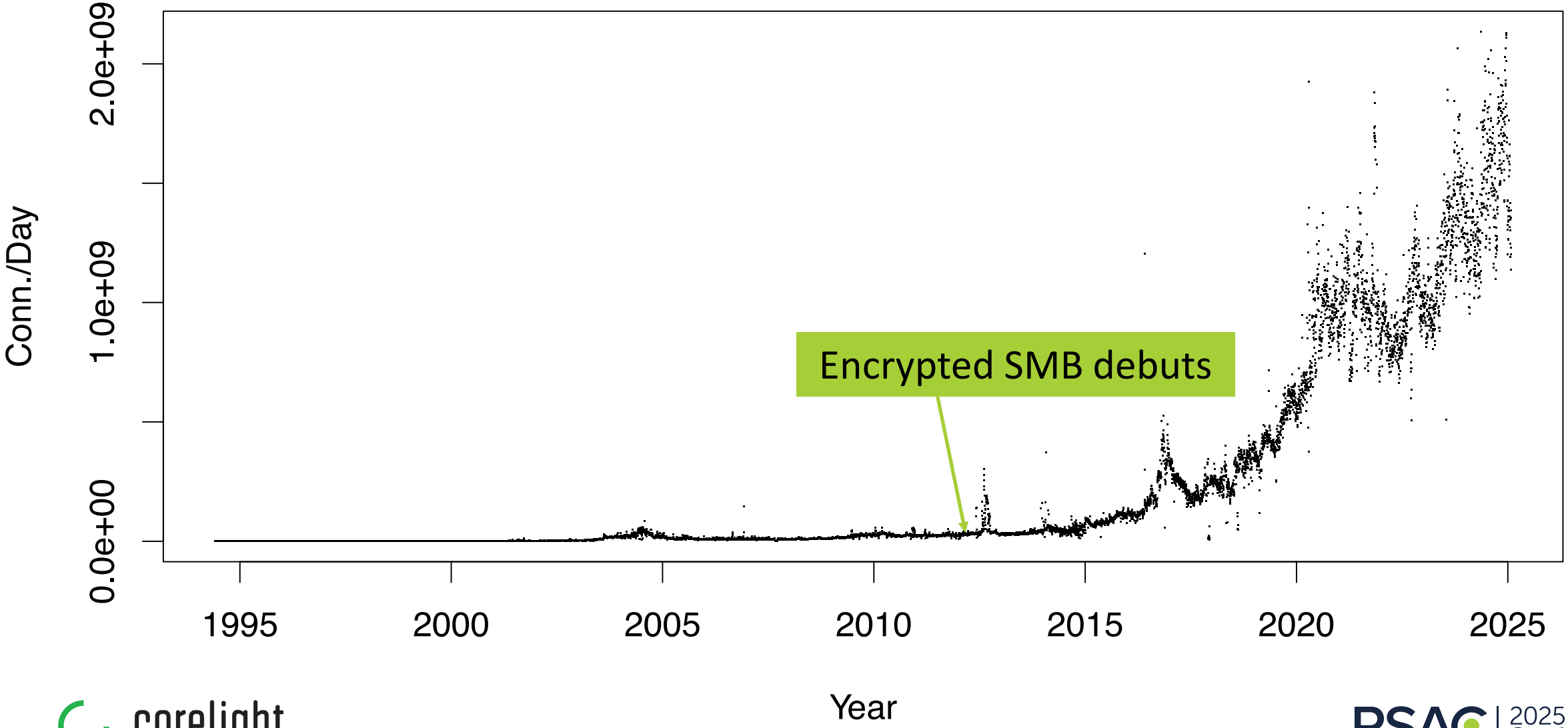
Evolution of Inbound Connections Per Day (LBNL)



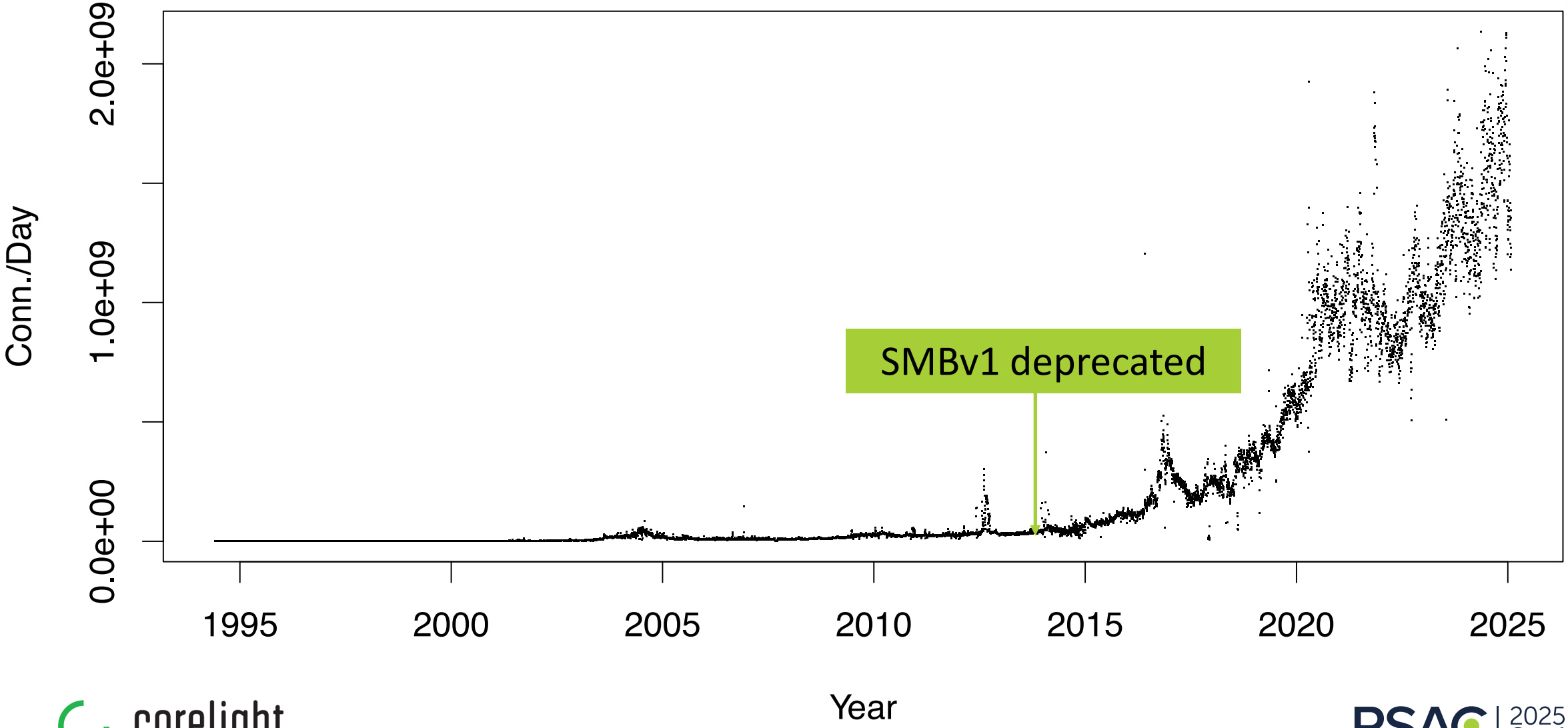
Evolution of Inbound Connections Per Day (LBNL)



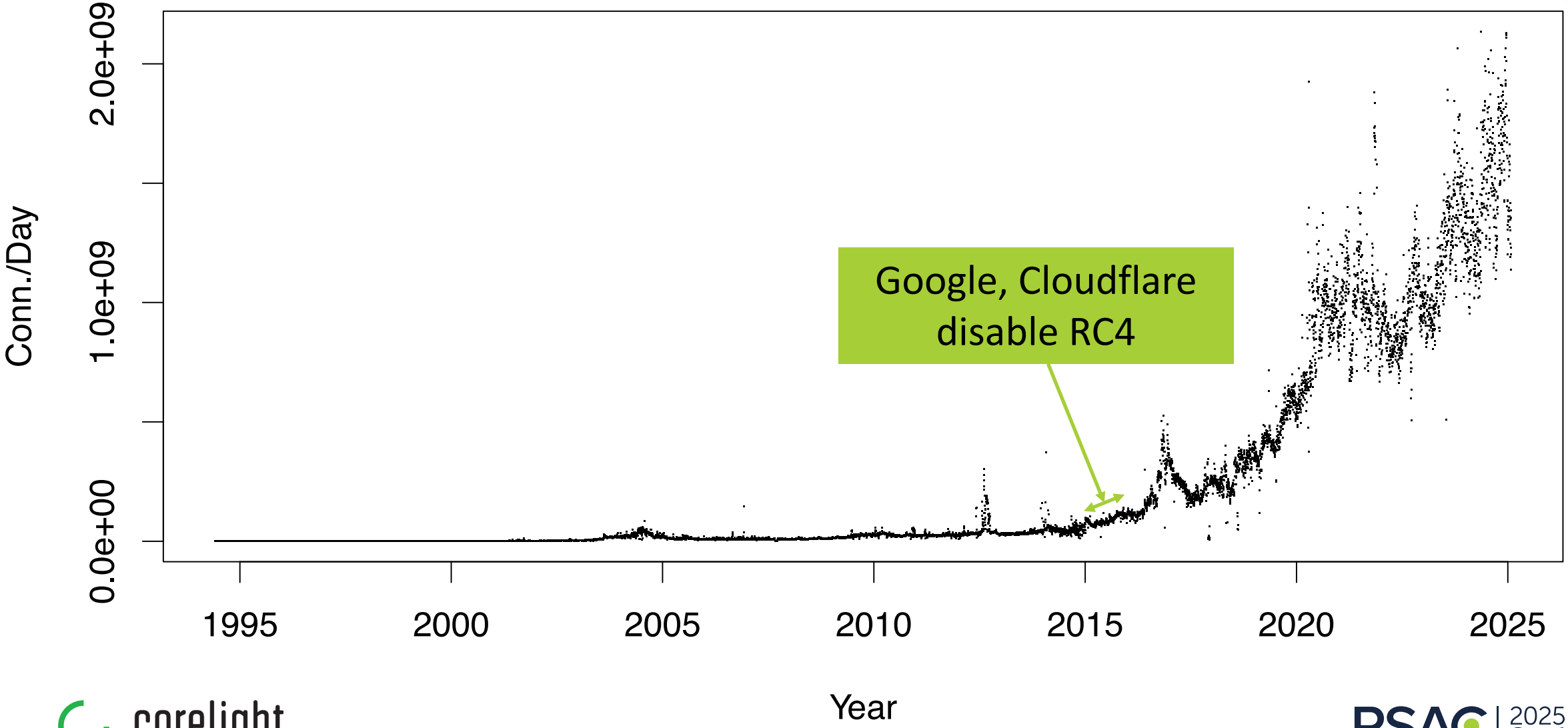
Evolution of Inbound Connections Per Day (LBNL)



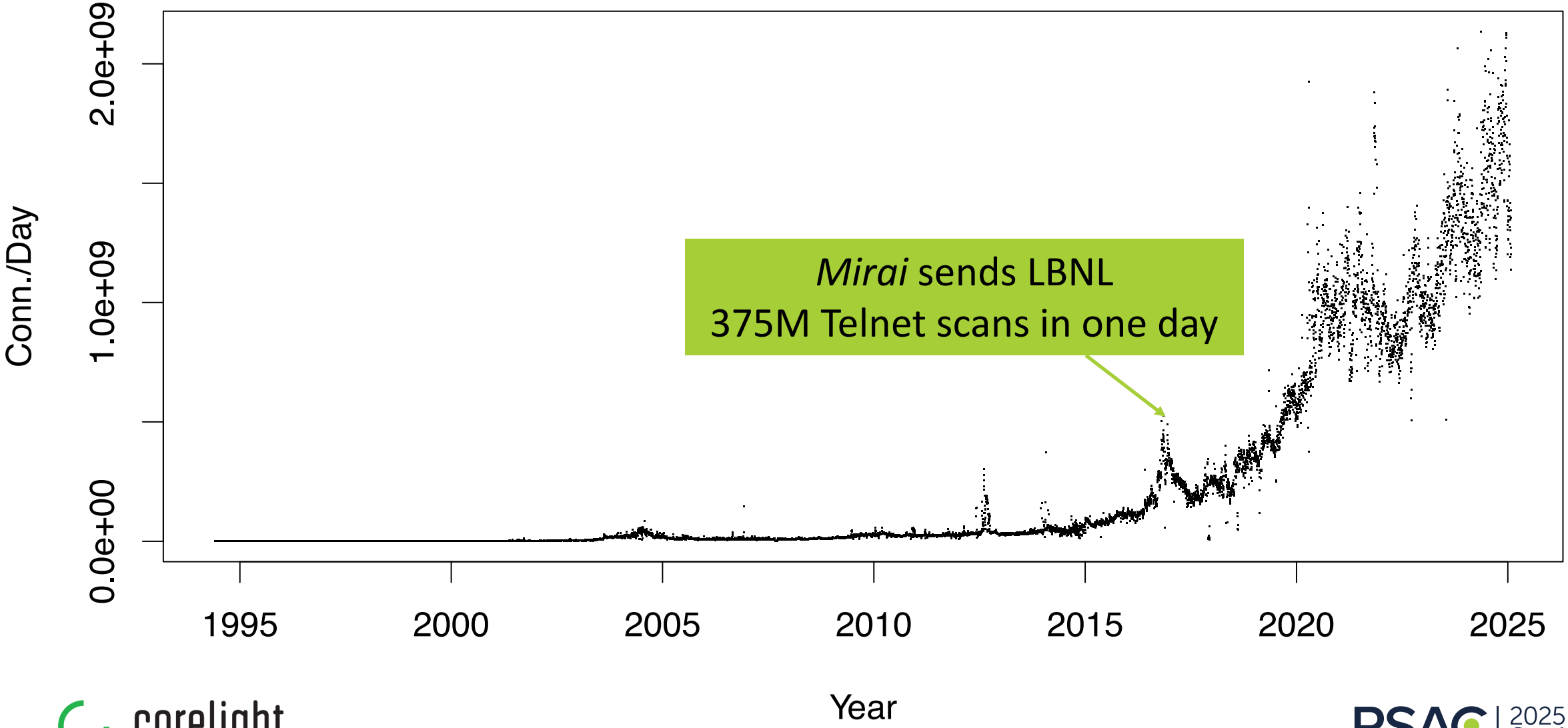
Evolution of Inbound Connections Per Day (LBNL)



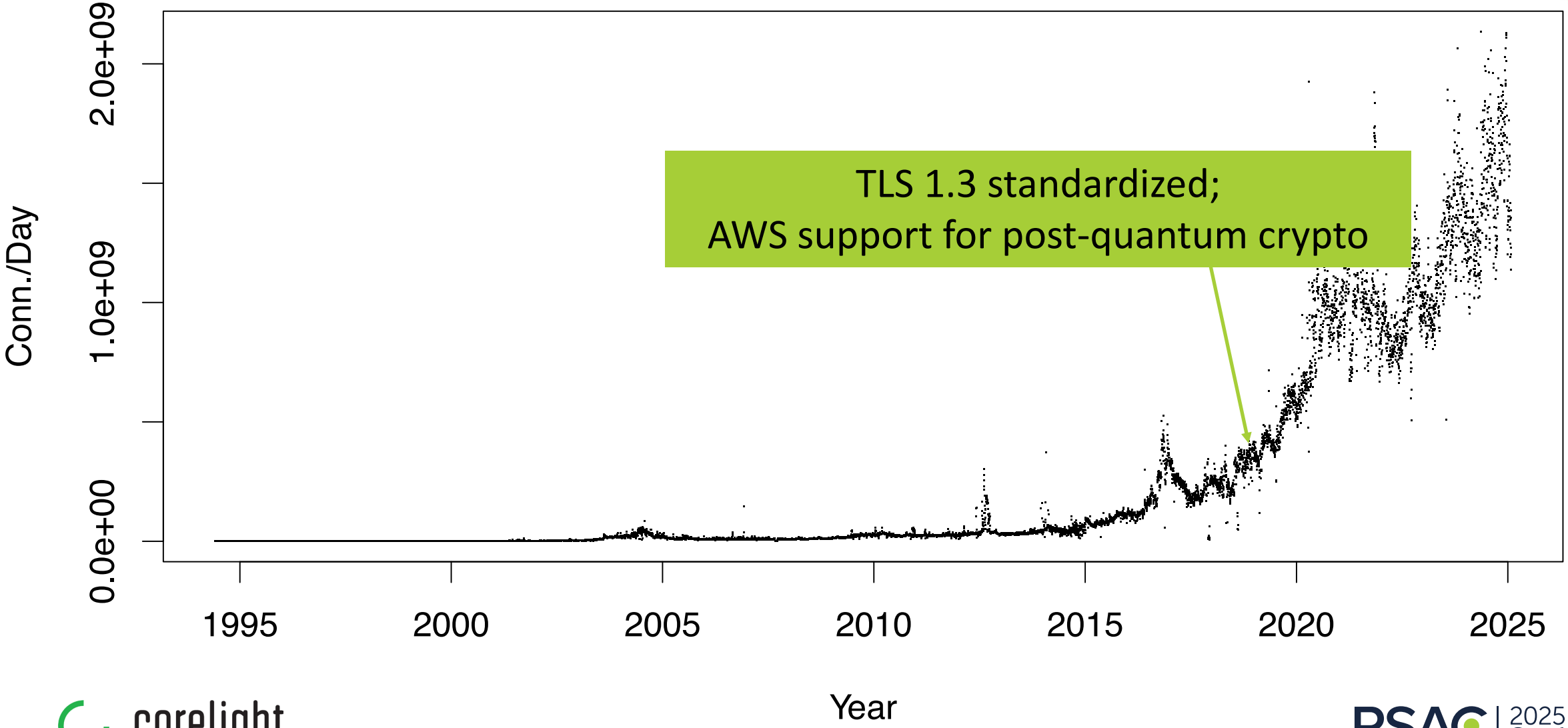
Evolution of Inbound Connections Per Day (LBNL)



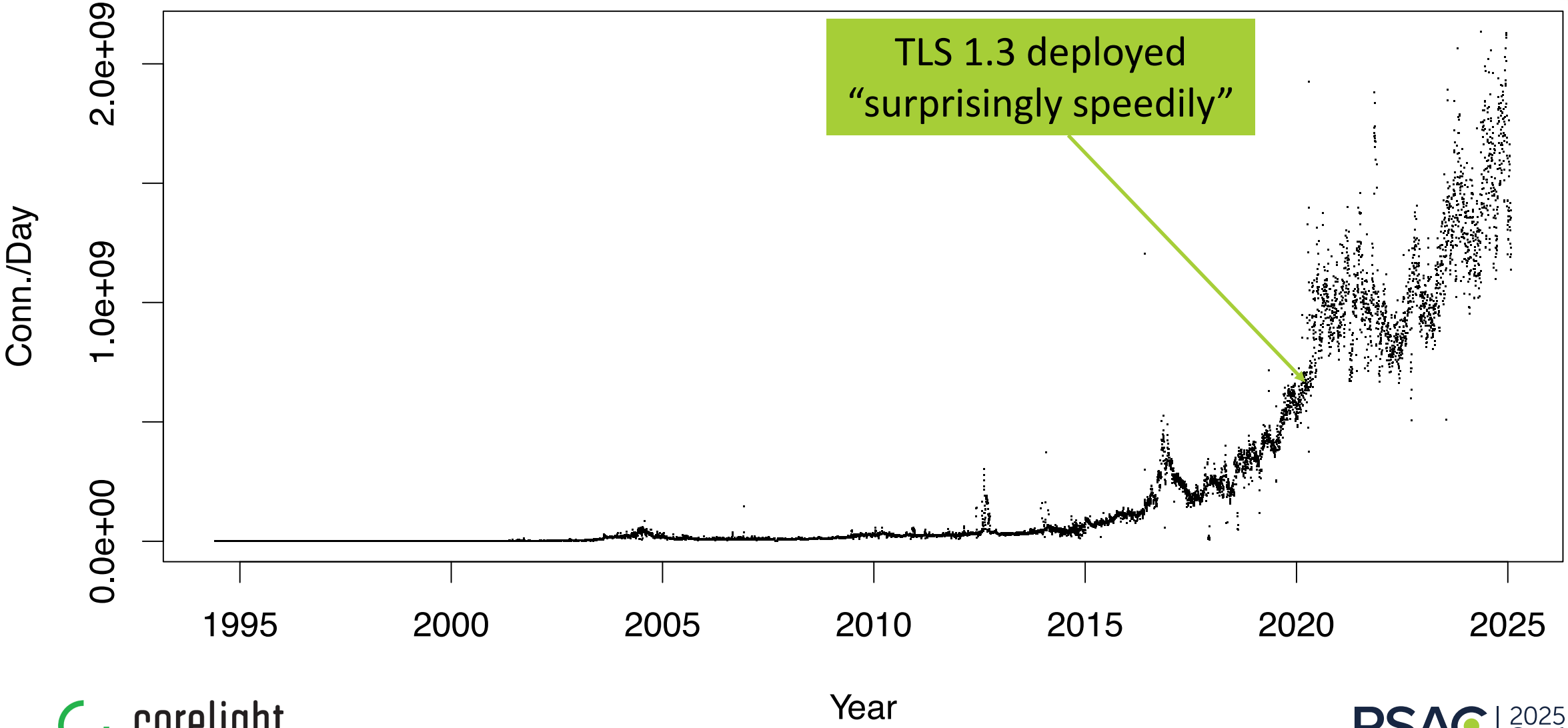
Evolution of Inbound Connections Per Day (LBNL)



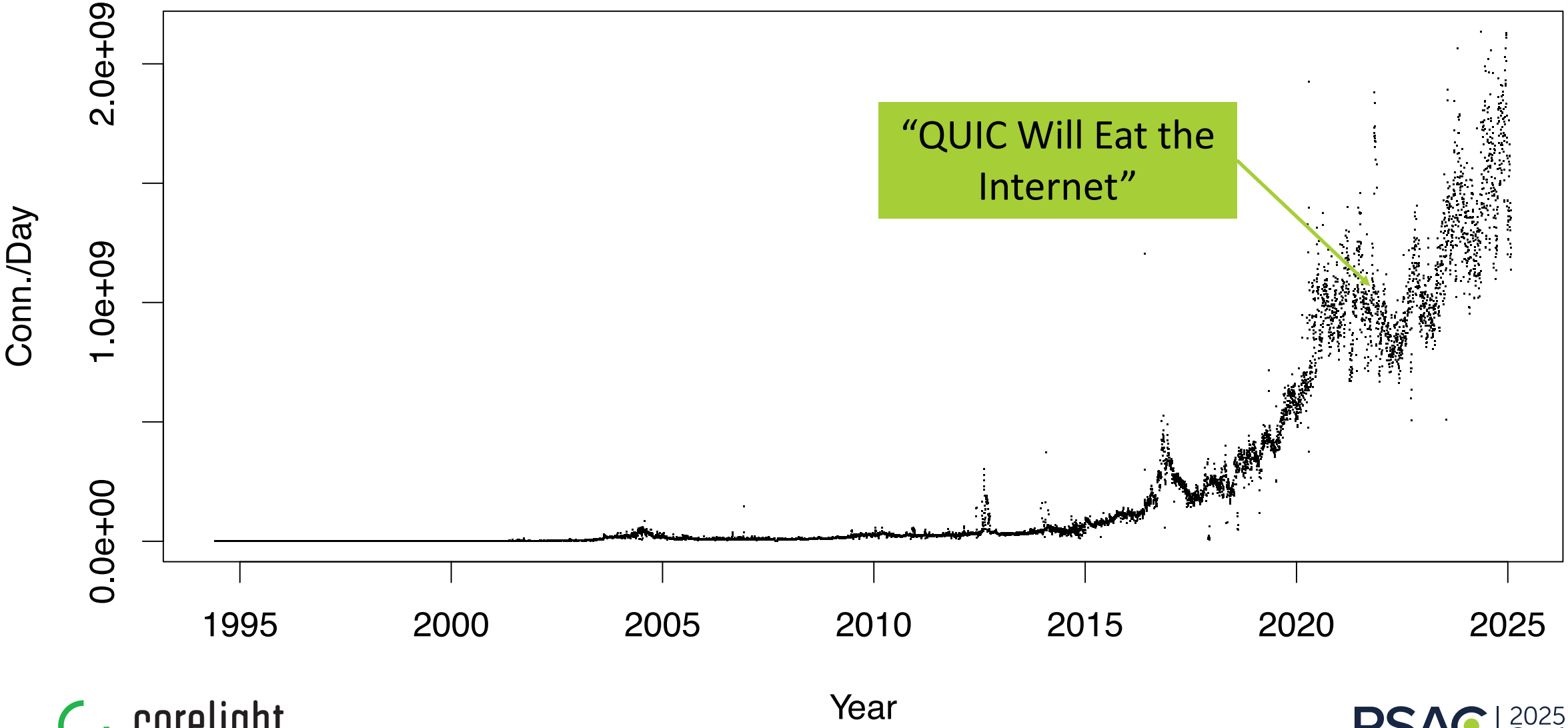
Evolution of Inbound Connections Per Day (LBNL)



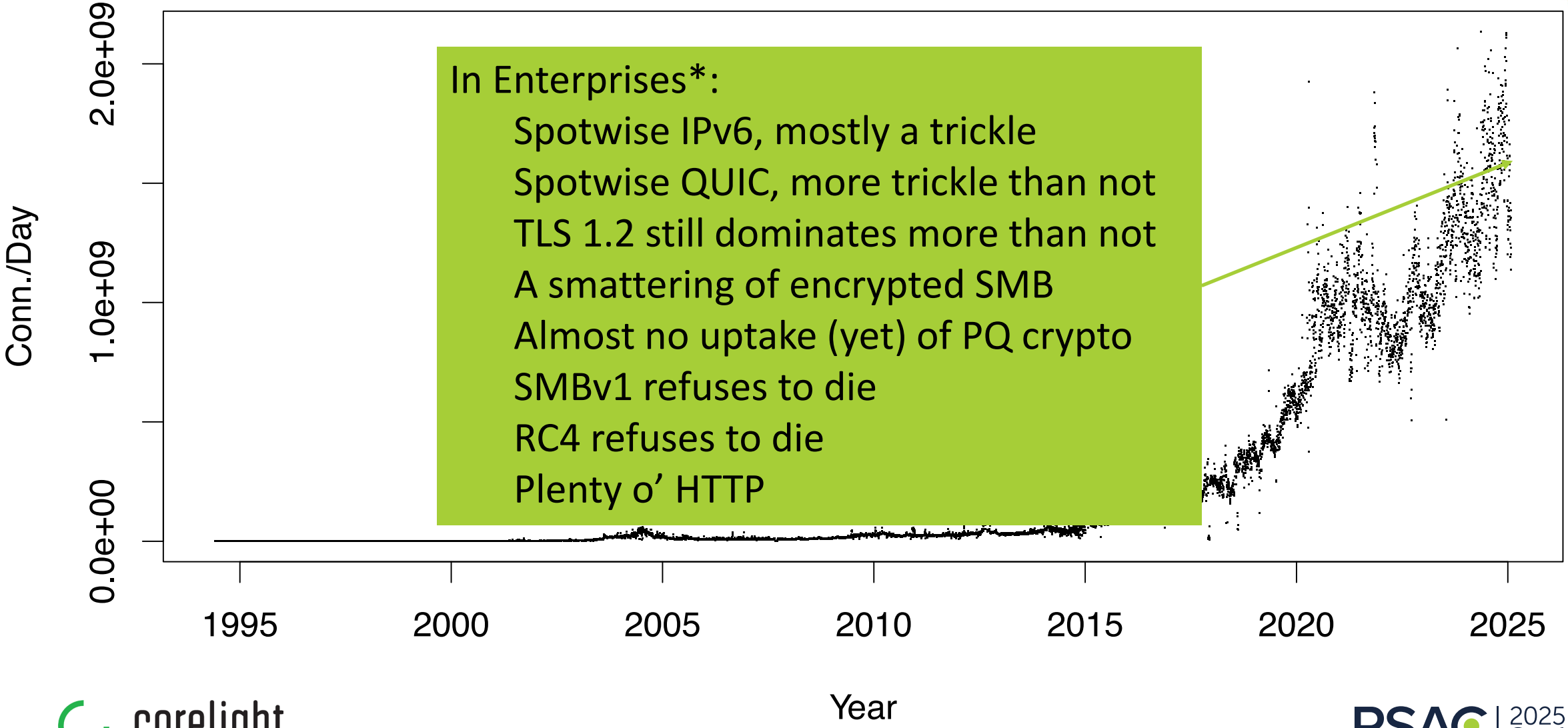
Evolution of Inbound Connections Per Day (LBNL)



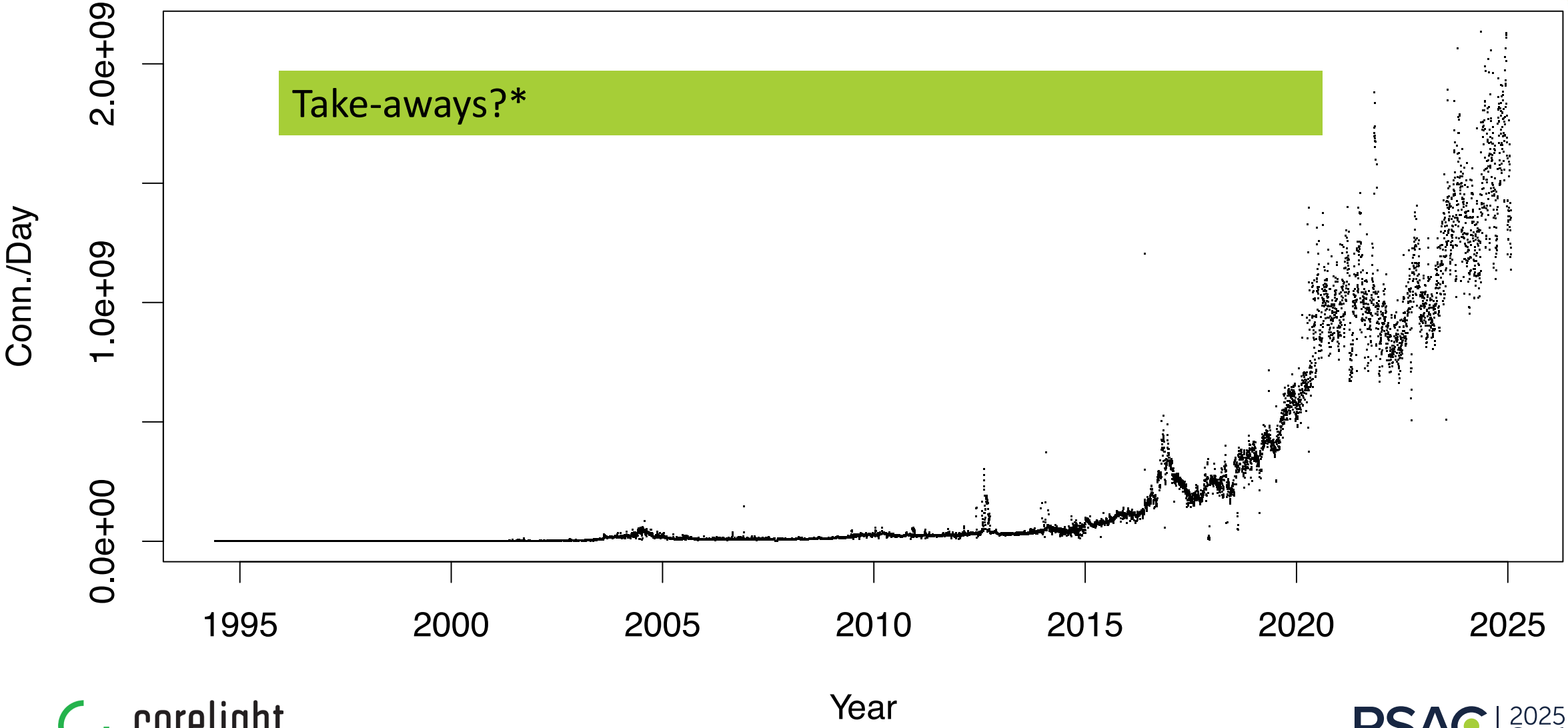
Evolution of Inbound Connections Per Day (LBNL)



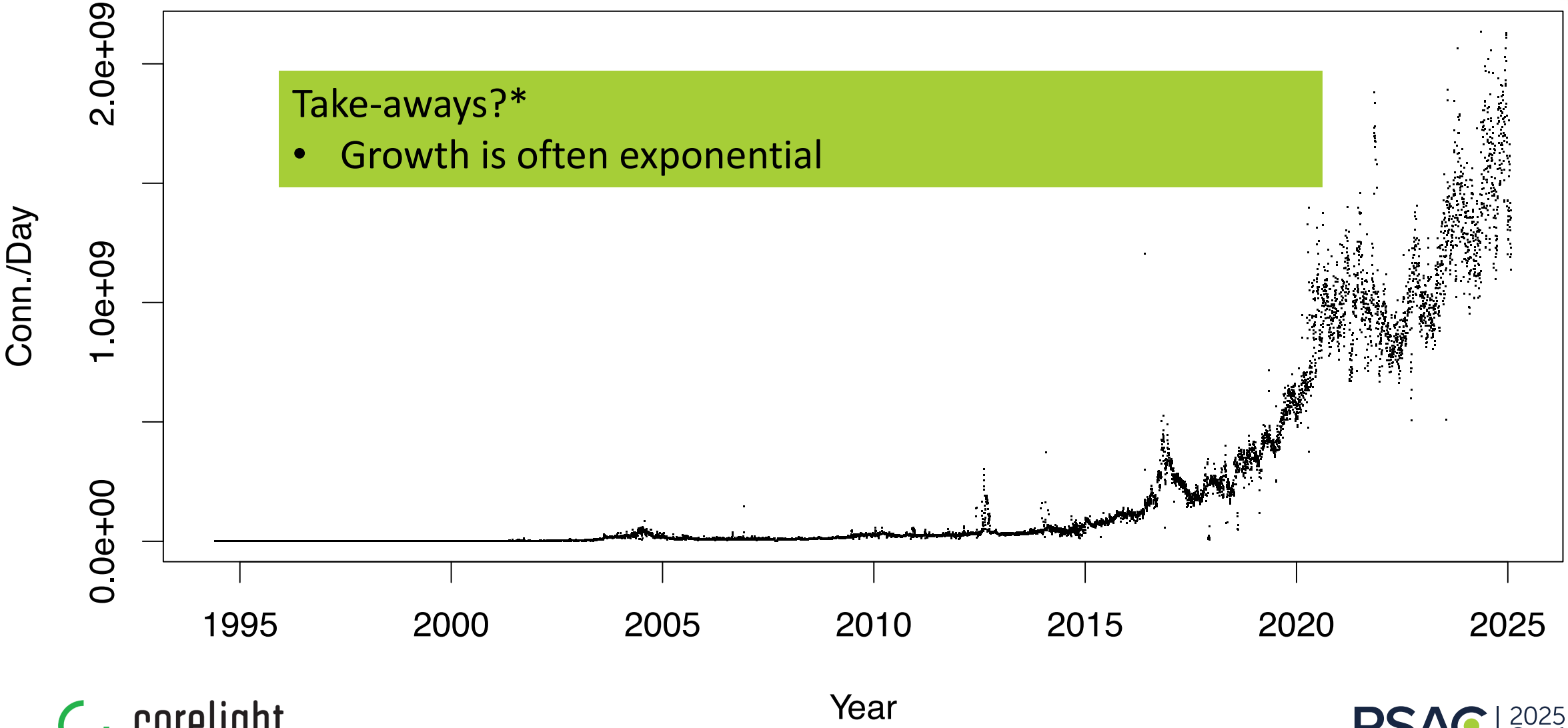
Evolution of Inbound Connections Per Day (LBNL)



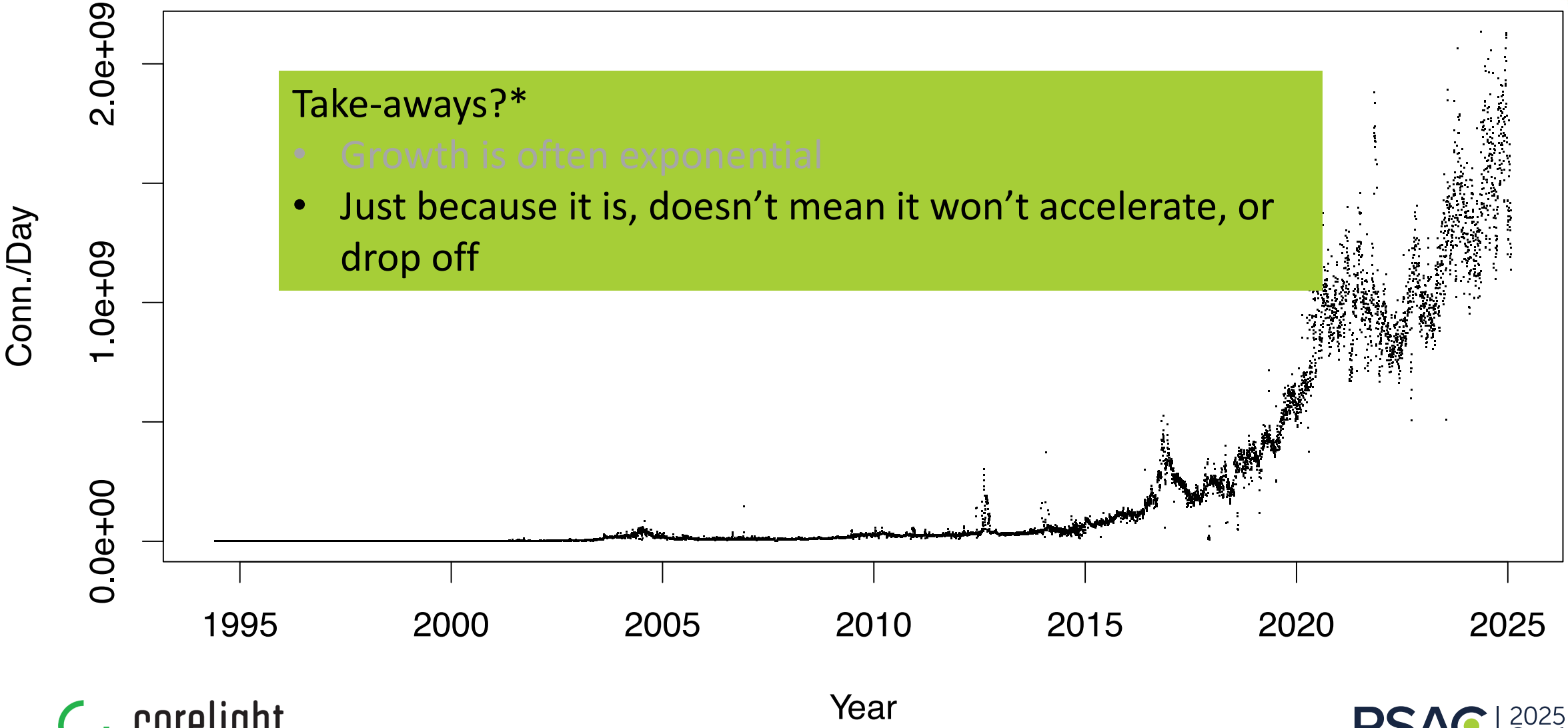
Evolution of Inbound Connections Per Day (LBNL)



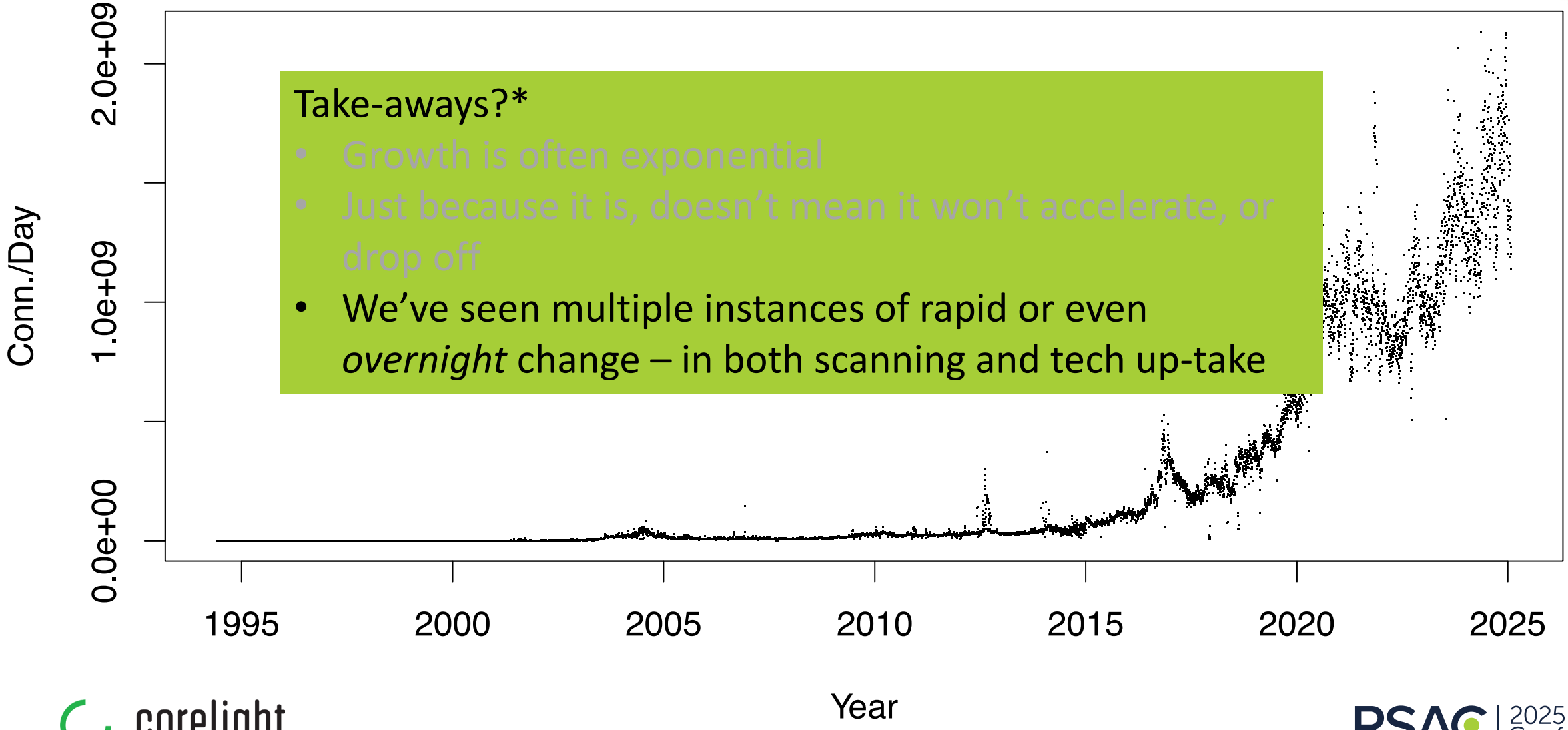
Evolution of Inbound Connections Per Day (LBNL)



Evolution of Inbound Connections Per Day (LBNL)



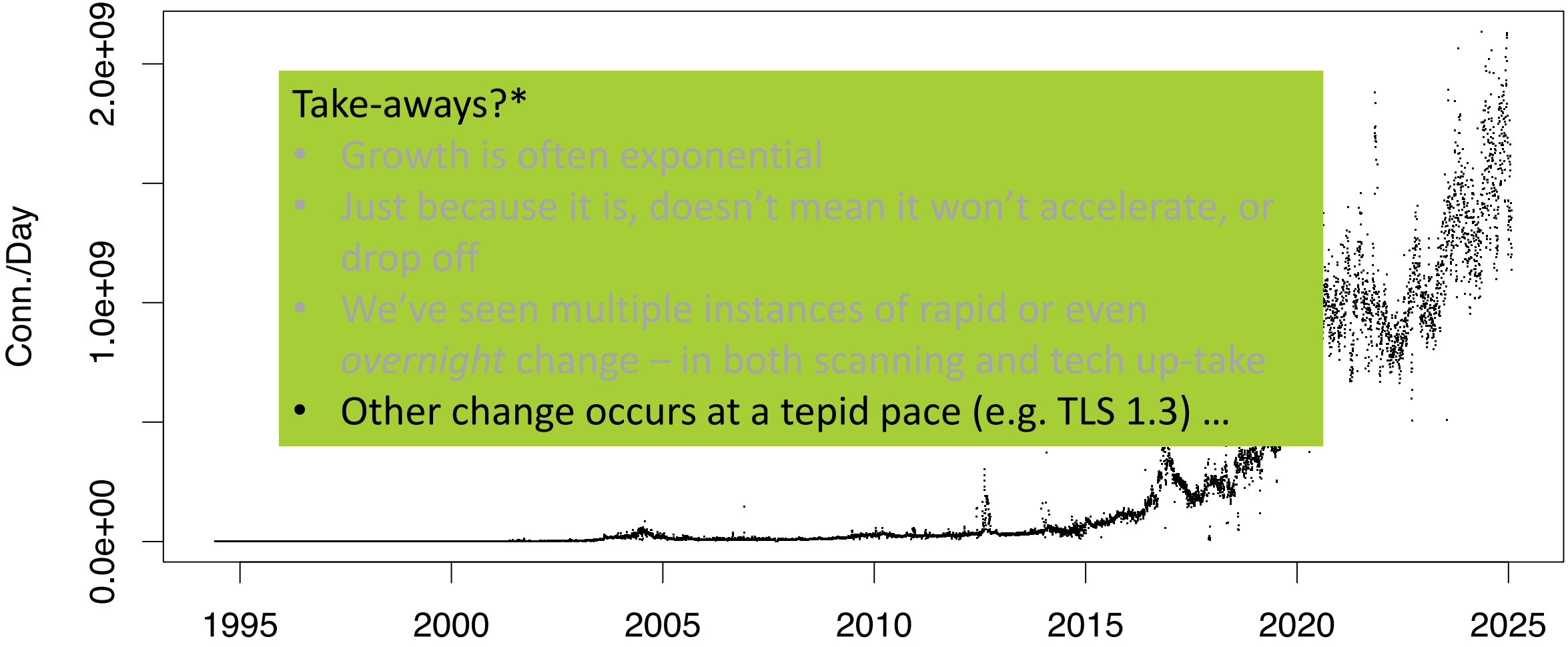
Evolution of Inbound Connections Per Day (LBNL)



Take-aways?*

- Growth is often exponential
- Just because it is, doesn't mean it won't accelerate, or drop off
- We've seen multiple instances of rapid or even *overnight* change – in both scanning and tech up-take

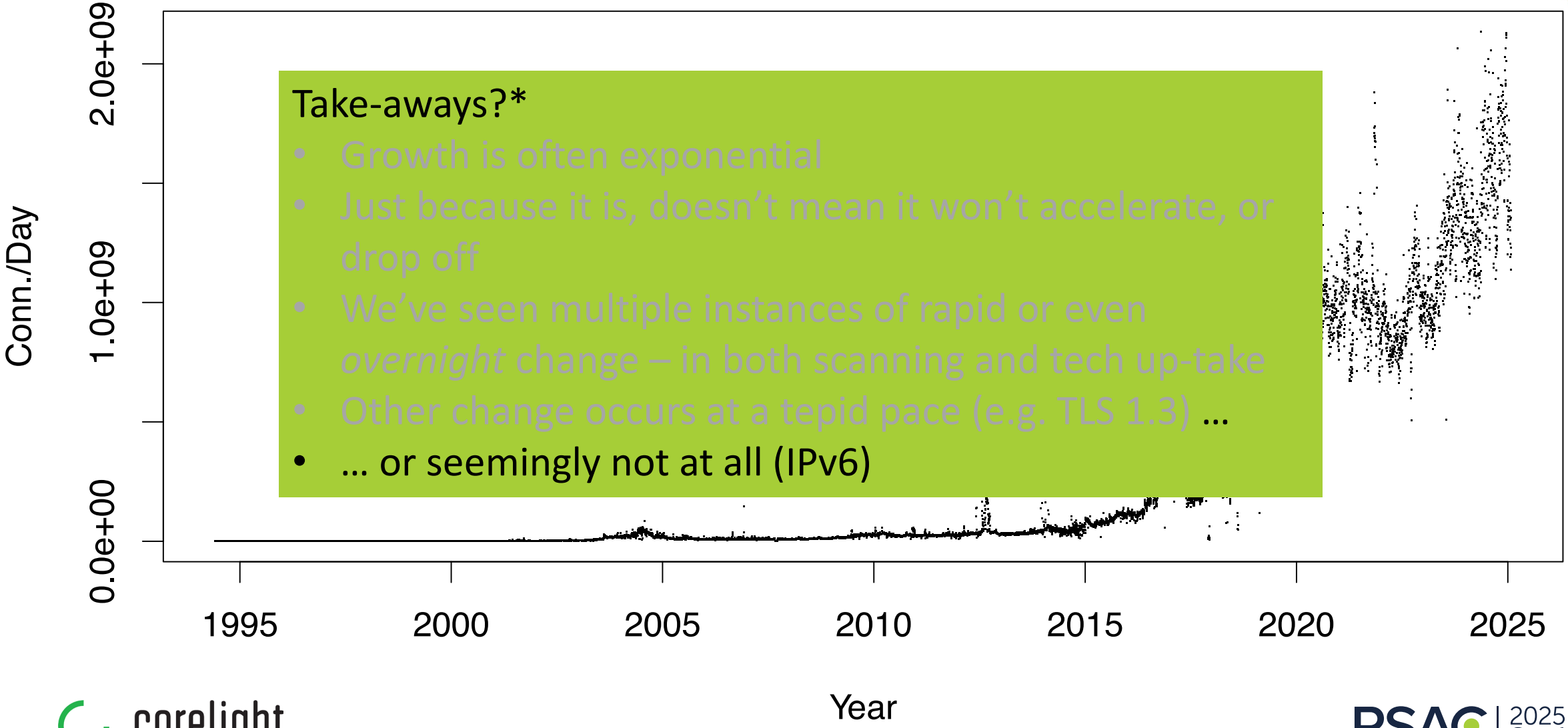
Evolution of Inbound Connections Per Day (LBNL)



Take-aways?*

- Growth is often exponential
- Just because it is, doesn't mean it won't accelerate, or drop off
- We've seen multiple instances of rapid or even *overnight* change – in both scanning and tech up-take
- Other change occurs at a tepid pace (e.g. TLS 1.3) …

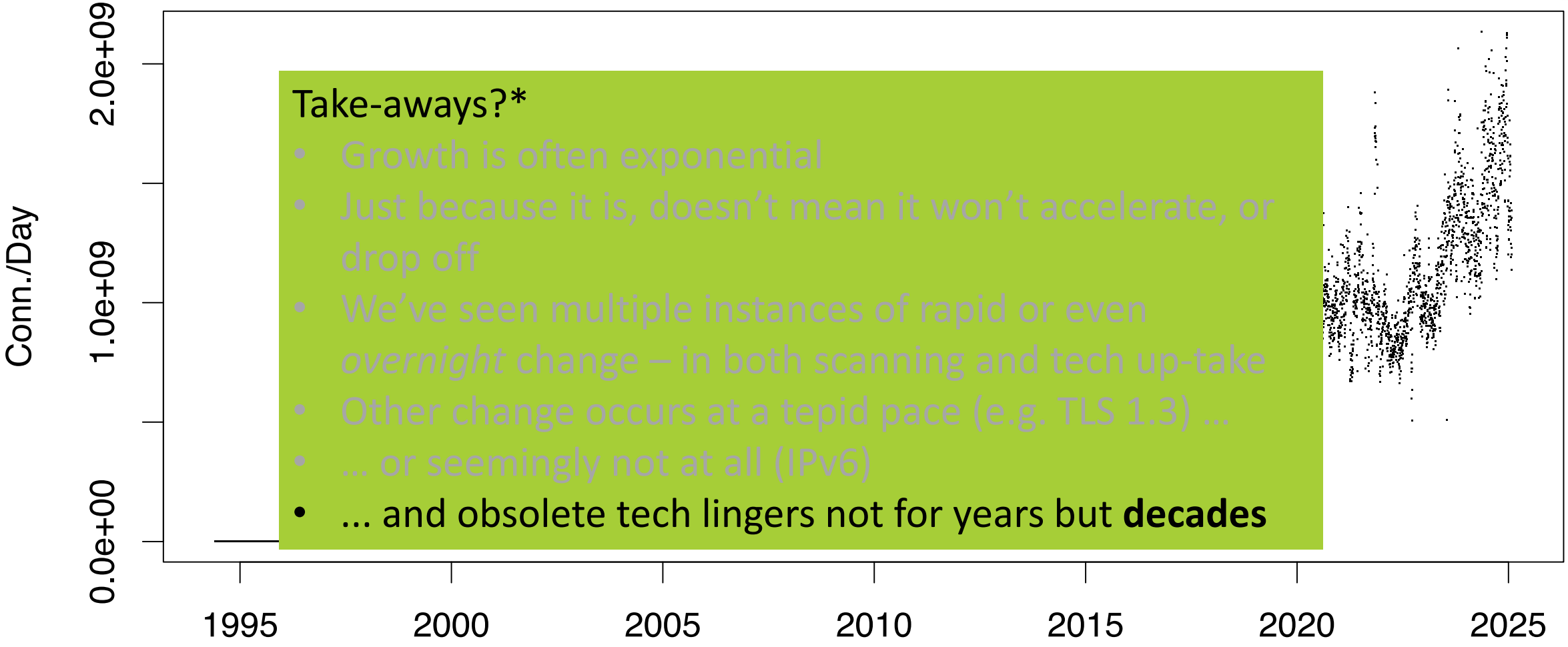
Evolution of Inbound Connections Per Day (LBNL)



Take-aways?*

- Growth is often exponential
- Just because it is, doesn't mean it won't accelerate, or drop off
- We've seen multiple instances of rapid or even *overnight* change – in both scanning and tech up-take
- Other change occurs at a tepid pace (e.g. TLS 1.3) …
- … or seemingly not at all (IPv6)

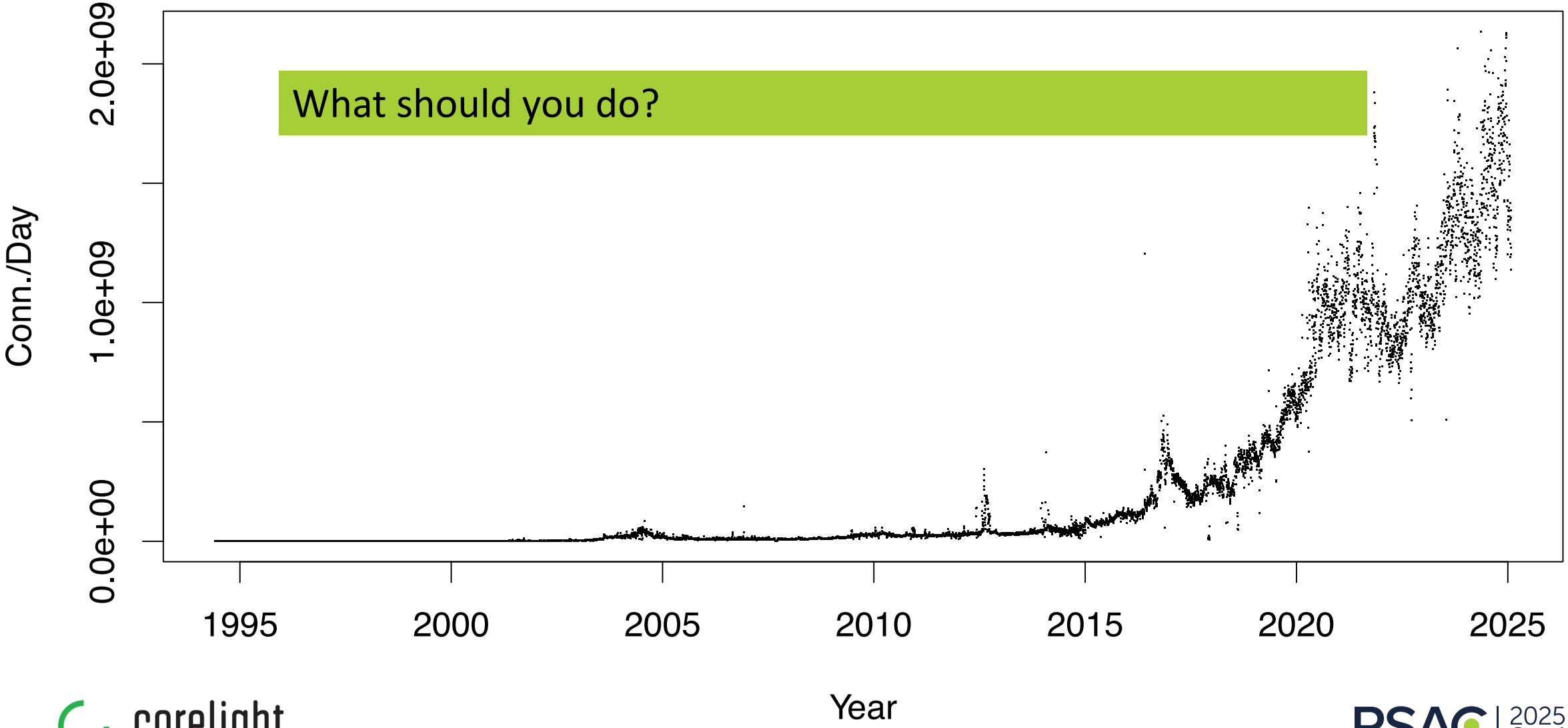
Evolution of Inbound Connections Per Day (LBNL)



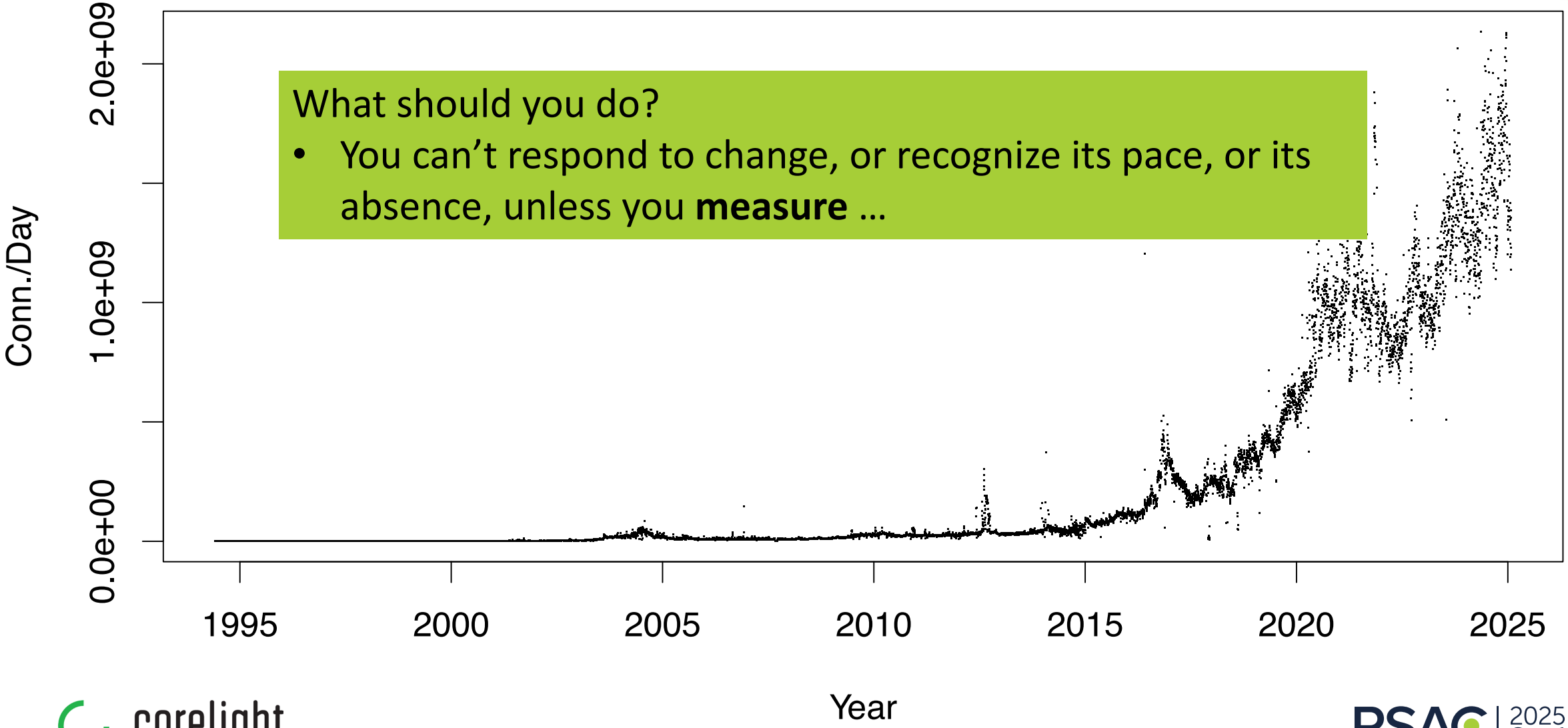
Take-aways?*

- Growth is often exponential
- Just because it is, doesn't mean it won't accelerate, or drop off
- We've seen multiple instances of rapid or even *overnight* change – in both scanning and tech up-take
- Other change occurs at a tepid pace (e.g. TLS 1.3) …
- … or seemingly not at all (IPv6)
- … and obsolete tech lingers not for years but **decades**

Evolution of Inbound Connections Per Day (LBNL)



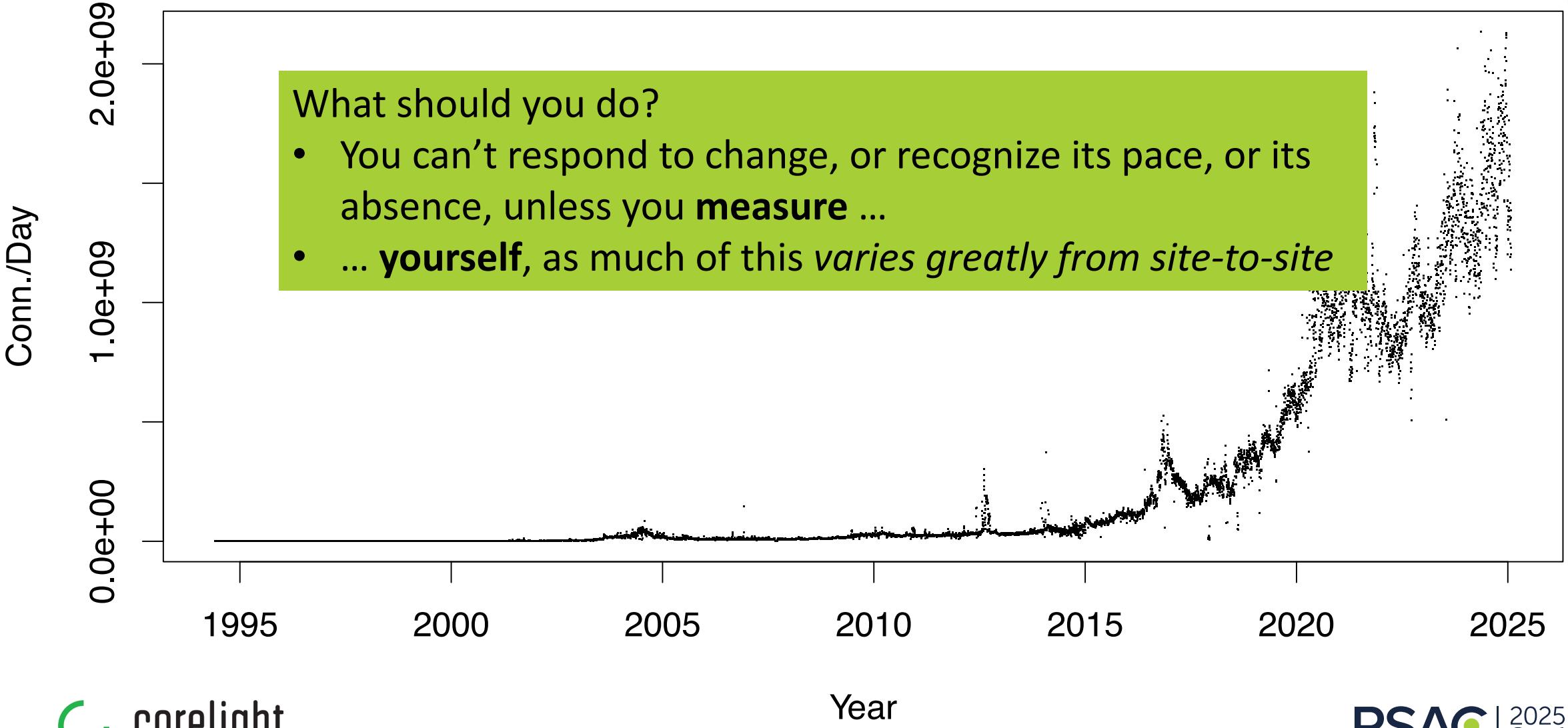
Evolution of Inbound Connections Per Day (LBNL)



What should you do?

- You can't respond to change, or recognize its pace, or its absence, unless you **measure** …

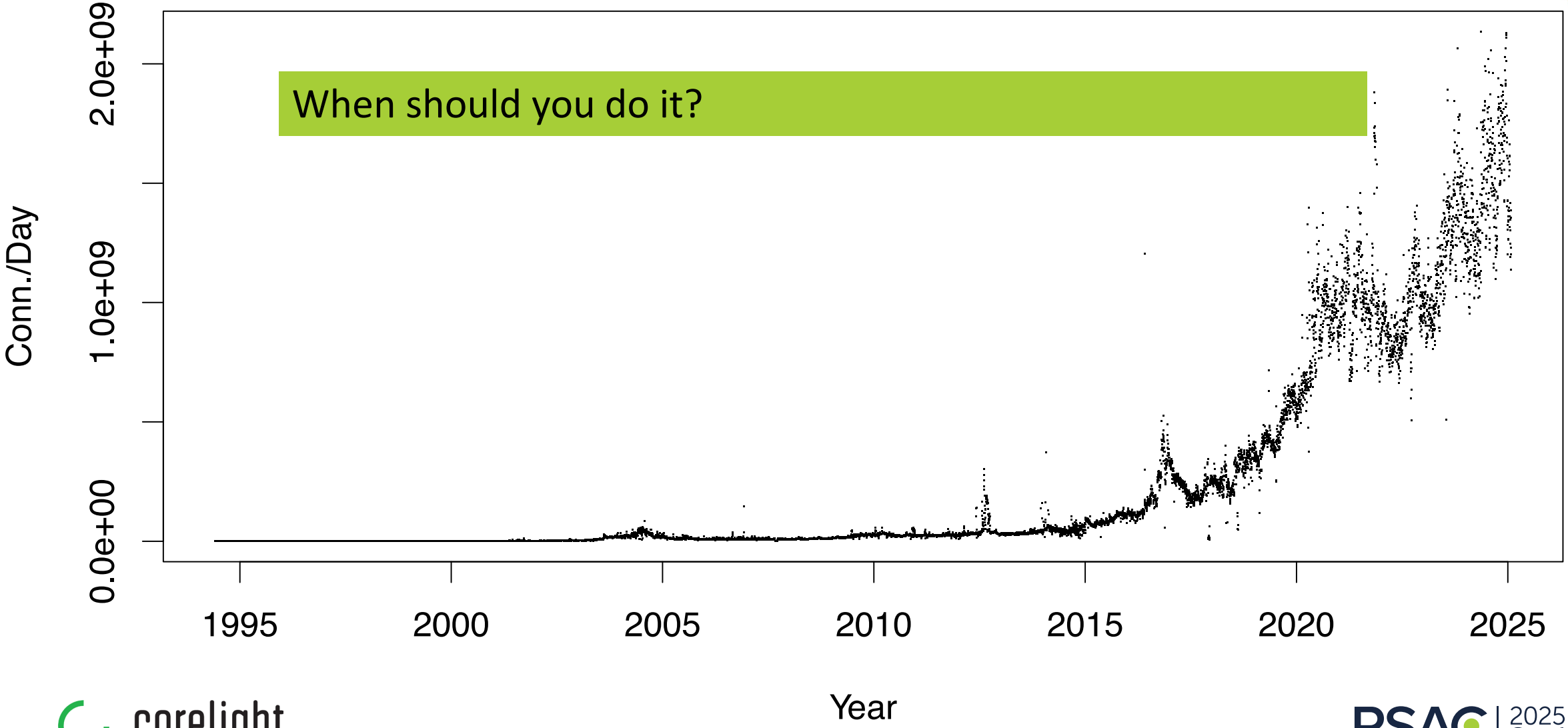
Evolution of Inbound Connections Per Day (LBNL)



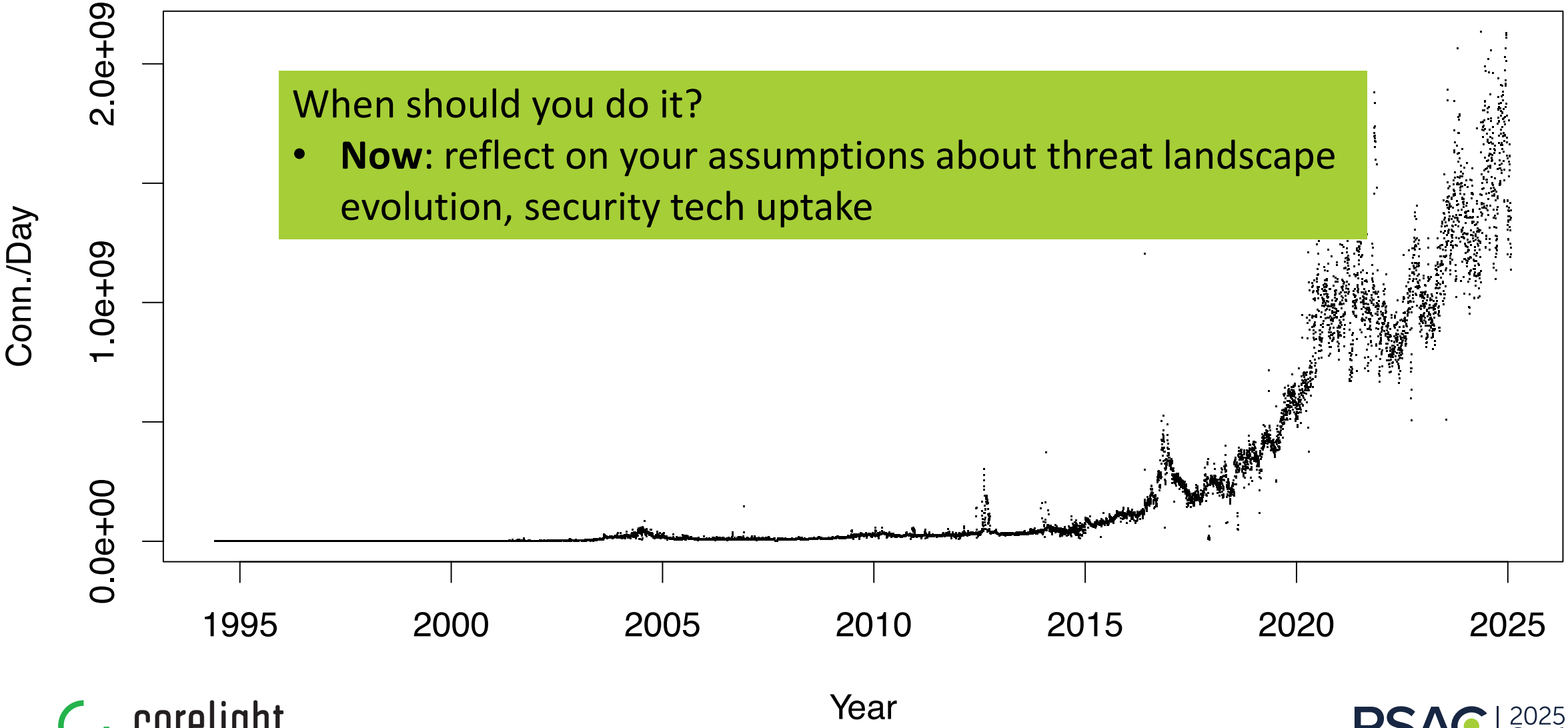
What should you do?

- You can't respond to change, or recognize its pace, or its absence, unless you **measure** …
- … **yourself**, as much of this *varies greatly from site-to-site*

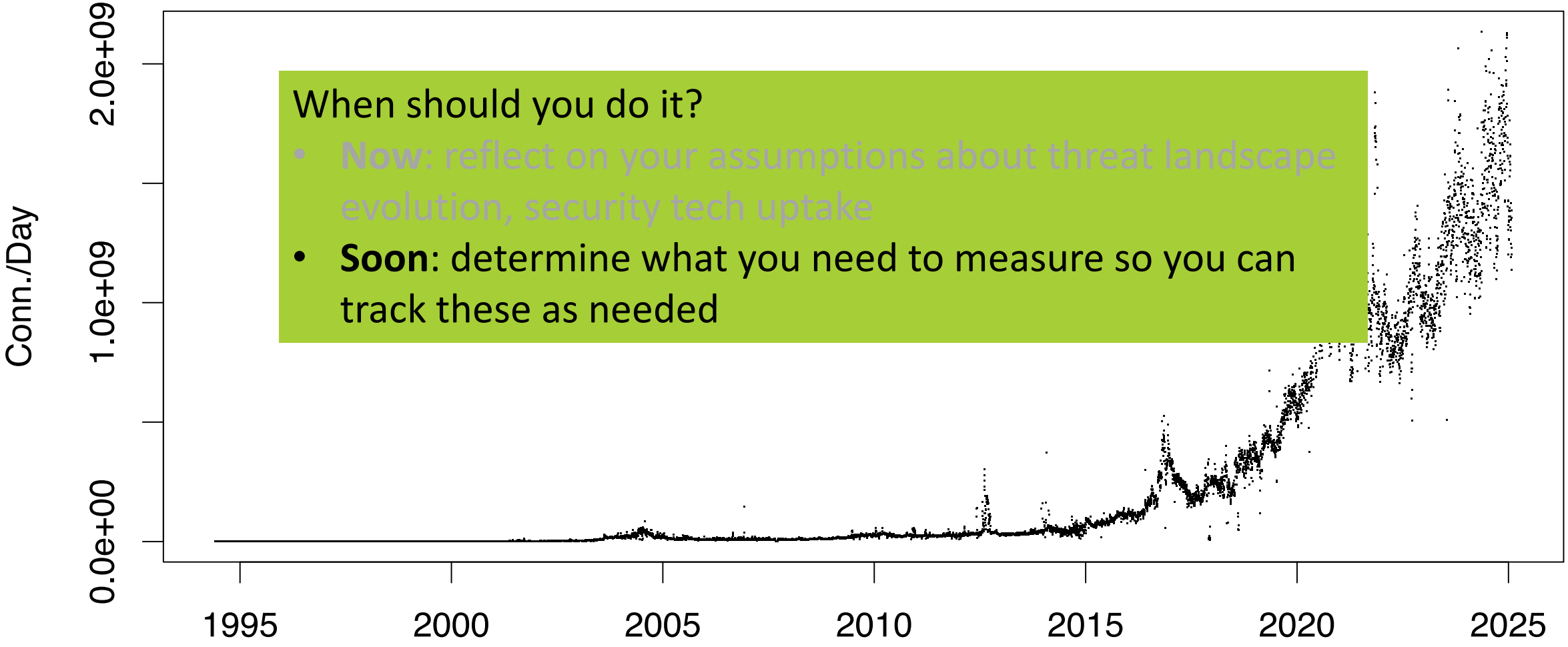
Evolution of Inbound Connections Per Day (LBNL)



Evolution of Inbound Connections Per Day (LBNL)



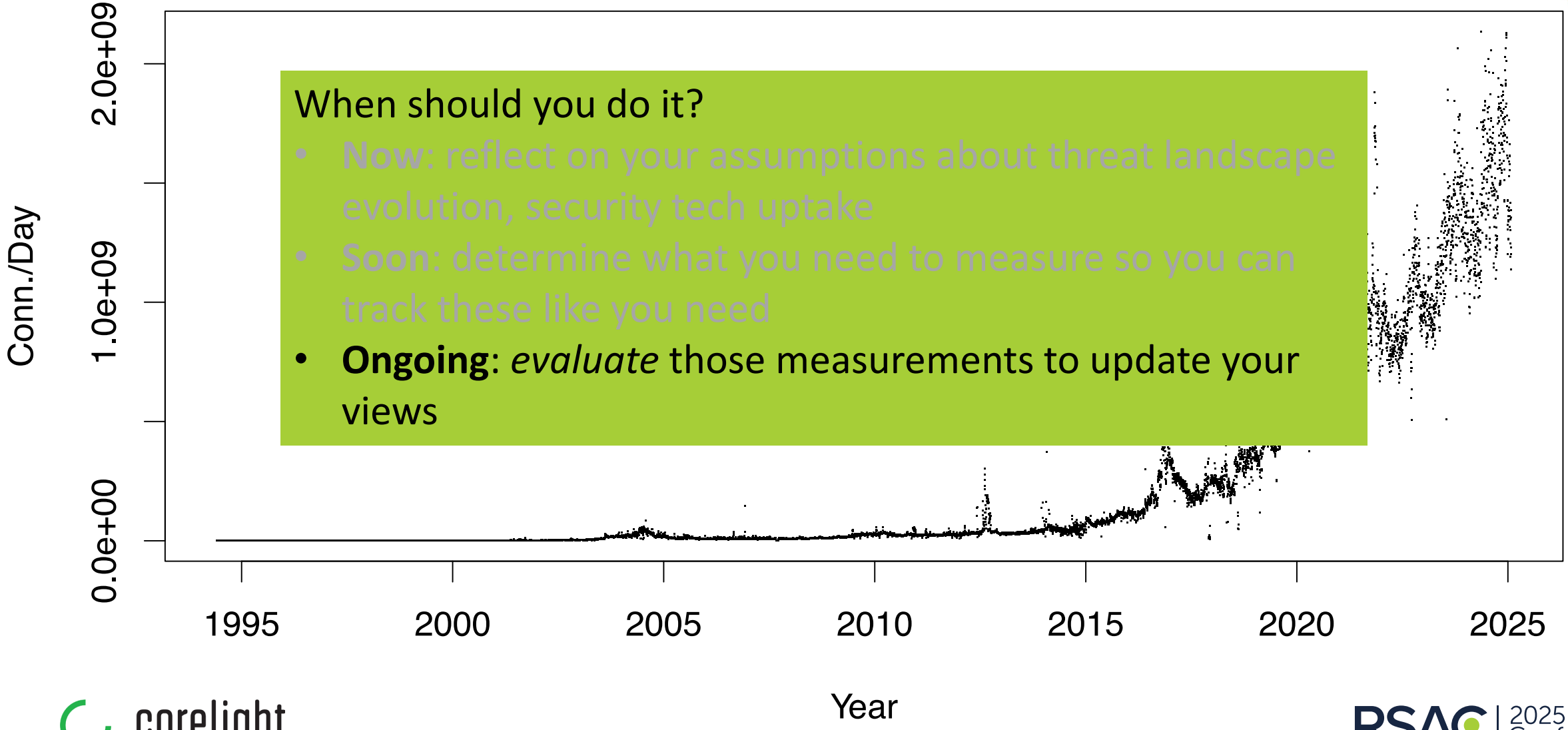
Evolution of Inbound Connections Per Day (LBNL)



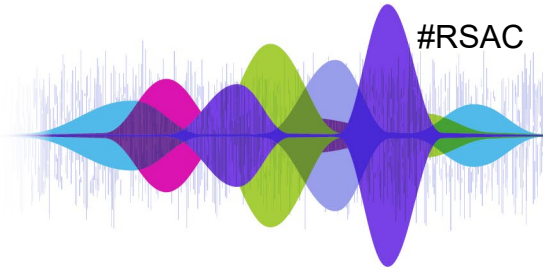
When should you do it?

- **Now**: reflect on your assumptions about threat landscape evolution, security tech uptake
- **Soon**: determine what you need to measure so you can track these as needed

Evolution of Inbound Connections Per Day (LBNL)



Apply What You Have Learned Today



- Next week you should:
  - Reflect on your assumptions about threat landscape evolution, security tech uptake
- In the first three months following this presentation you should:
  - Determine what you need to measure so you can track these as needed
  - Implement associated measurement processes
- Within six months you should:
  - Establish processes for ongoing analysis of measurements
  - Revisit your assumptions in light of what the analysis shows

RSAC 2025 Conference

Many Voices.
One Community.

Vern Paxson, Co-Founder and Chief Scientist, Corelight Inc.

Professor of the Graduate School, UC Berkeley

vern@corelight.com / vern@berkeley.edu